Pontifícia Universidade Católica
do Rio de Janeiro

Frederico Boghossian Torres

Proteção de dados nas cidades inteligentes

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Direito do Estado e Teoria Constitucional pelo Programa de Pós-Graduação em Direito, do Departamento de Direito da PUC-Rio.

Orientadora: Caitlin Sampaio Mulholland

Rio de Janeiro,

maio de 2022

Pontifícia Universidade Católica
do Rio de Janeiro

Frederico Boghossian Torres

Proteção de Dados nas Cidades Inteligentes

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Direito do Estado e Teoria Constitucional pelo Programa de Pós-Graduação em Direito, do Departamento de Direito da PUC-Rio.
Aprovado pela Comissão Examinadora abaixo:

Profª. Caitlin Sampaio Mulholland
Orientadora
Departamento de Direito – PUC-Rio

Profª. Virgínia Totti Guimarães
Departamento de Direito – PUC-Rio

Prof. Carlos Affonso Pereira de Souza
PUC-Rio

Rio de Janeiro, 23 de maio de 2022

Frederico Boghossian Torres

Graduou-se em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). É pesquisador e advogado especialista em temas de proteção de dados e regulação de novas tecnologias. Membro da Clínica de Direitos Fundamentais da UERJ e do Legalite, núcleo multidisciplinar de Legal Informatics integrado ao Departamento de Direito da PUC-Rio.

Ficha Catalográfica

Torres, Frederico Boghossian

Proteção de dados nas cidades inteligentes / Frederico Boghossian Torres; orientadora: Caitlin Sampaio Mulholland. – 2022.

146 f. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Direito, 2022.

Inclui bibliografia

1. Direito – Teses. 2. Cidades inteligentes. 3. Proteção de dados. 4. Privacidade. 5. Segurança da informação. 6. Direito à cidade. I. Mulholland, Caitlin Sampaio. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Direito. III. Título.

CDD:340

Ao que sonham com cidades ainda invisíveis.

Agradecimentos

Escrever não é tarefa fácil. O resultado formatado, as frases conectadas, o início, o meio e o fim. Nada disso deixa transparecer as páginas lidas, as idas e vindas com o tema e as noites mal dormidas. O mais fácil de escrever é o ato final: caneta no papel e dedo nas teclas. Mas, até aí, a história tem muitas cenas: o autoquestionamento, a vontade de desistir e o contínuo trabalho.

Mas a peça tem final feliz. O tempo passa, o prazo aperta e as ideias saem. Quando menos se espera, há um rascunho que vira dissertação. E esse processo é um caminho de crescimento que vai muito além da pesquisa. Pesquisar é ter coragem de pôr o cérebro e o coração no palco e descobrir o quanto você precisa estudar. E essa coragem ninguém constrói sozinho.

Em primeiro, agradeço à minha esposa, Bianca, por me manter de cabeça e coração saudáveis nessa caminhada. Foram muitos fins de semana de trabalho, programas perdidos e de dedicação. Sem a compreensão de quem se ama, o caminho teria sido muito mais difícil. Obrigado por aguentar a ansiedade e o mau humor de quem pesquisa.

À minha família, obrigado por tudo que fazem por mim. Somos parte uns dos outros e vivemos uns para os outros. Logo antes do mestrado, eu não sabia o que seria de mim, mas vocês nunca tiveram dúvida e, por isso, me encheram de amor e confiança. Anita, Guilherme, Paula e João Pedro: a vocês eu devo tudo.

Agradeço à Profª. Caitlin, por ter escolhido um texto sobre proteção de dados para a seleção de mestrado, criando em mim a curiosidade sobre um tema que virou paixão e trajetória profissional. É um privilégio ser seu orientando e ter a chance de trocar perguntas e risadas com uma pessoa tão qualificada e amiga.

É também um privilégio ser parte do Legalité, onde tive a oportunidade de conhecer pessoas e pesquisadores incríveis, como o Samuel, o Pedro, a Paula, a Hana, o Marcos e a Bianca, com quem aprendo a cada dia. A estes e todos os demais membros: muito obrigado!

Sou muito grato ao Departamento de Direito da PUC-Rio, que me deu a oportunidade de rir e chorar enquanto me tornava acadêmico. O carrossel do

mestrado, com uma semana de aula presencial até o início de uma pandemia que suspenderia os encontros por dois anos, foi uma viagem que me marcou.

Nada disso teria sido possível sem minha turma, que enfrentou as incertezas da pandemia, das novas formas de ensino e dos cortes no orçamento da pesquisa nacional. Muito se ouve sobre briga de egos e rivalidade na academia e, se isso é verdade, eu não presenciei. Por isso, sou grato aos meus colegas que tanto apoio me deram. Um abraço especial à Ticiana, ao Lucas, ao Cadu, à Natasha e à Luisa, que ouviram minhas reclamações e dúvidas com tanta paciência.

Deixo meus agradecimentos, também, aos companheiros de profissão, que tanto me ensinam sobre a prática em proteção de dados. Aos eternos chefes, Samanta, Daniel e Beatriz: muito obrigado! Aos companheiros argentinos, Pablo, Belu, Lucho, Melisa y Juan: ¡*muchas gracias*!

Por fim, agradeço à Cátia, que nos últimos dois anos me ajudou a encontrar forças que eu não sabia ter e a descobrir quem sou e quem quero ser.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Resumo

Torres, Frederico Boghossian; Mulholland, Caitlin Sampaio. **Proteção de dados nas cidades inteligentes**. Rio de Janeiro, 2022. 146p. Dissertação de Mestrado – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro.

As cidades contemporâneas, cuja população está em tendência de crescimento, são palco dos desafios do presente, como as mudanças climáticas, o acesso a alimentos, os desastres ambientais, o consumo de energia e emissão de gases poluentes, a violência, a desigualdade social, entre outros. A solução desses problemas é complexa e necessita o envolvimento de múltiplos atores e o investimento de volumosos recursos financeiros. Com atenção a isso, surge o ideal da cidade inteligente, que busca utilizar as tecnologias da informação e comunicação para diagnosticar e enfrentar problemas urbanos a partir da coleta e uso de dados sobre a cidade e os cidadãos. Se, por um lado, a tecnologia pode e deve ser utilizada para a melhoria da qualidade de vida, por outro lado, o seu uso traz dúvidas sobre a violação da privacidade dos cidadãos. Por estes motivos, a presente pesquisa objetiva estudar de que forma é possível realizar as promessas da cidade inteligente sem que isso signifique a expansão da vigilância e a sistematização da violação às leis de proteção de dados. Para isso, o trabalho irá: estudar as definições do conceito de cidade inteligente, abordar os desafios para a proteção de dados neste contexto e propor medidas que mitiguem os danos à privacidade dos cidadãos.

Palavras-chave

Cidades inteligentes; proteção de dados; privacidade; segurança da informação; direito à cidade; dados pessoais;

Abstract

Torres, Frederico Boghossian; Mulholland, Caitlin Sampaio(Abstract). **Data protection in the smart cities**. Rio de Janeiro, 2022. 146p. Dissertação de Mestrado – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro.

Contemporary cities, whose population is on a growing trend, are the main stage for the challenges of the present, such as climate change, access to food, environmental disasters, energy consumption and the emission of greenhouse gases, violence, social inequality, among others. The solution of these problems is complex, requiring the involvement of multiple actors and the investment of voluminous financial resources. With this in mind, the ideal of the smart city emerges, seeking to use information and communication technologies to diagnose and address urban problems by collecting and processing data about the city and its citizens. If, on the one hand, technology can and should be used to improve the quality of life, on the other hand, its use raises doubts about the violation of citizens' privacy. For these reasons, the present research aims to study how it is possible to fulfill the promises of the smart city without this meaning the expansion of surveillance and the systematization of violations of data protection laws. For this, the work will: study the definitions of smart city, address the challenges for data protection in this context and propose measures that mitigate the damages to the privacy of urban citizens.

Keywords

Smart cities; data protection; privacy; information security; right to the city; personal data; LGPD; GDPR.

Sumário

Lista de figuras e tabelas

Lista de Abreviaturas e Siglas

AEPD – Agencia Española de Protección de Datos

ANPD – Autoridade Nacional de Proteção de Dados

CBCI – Carta Brasileira de Cidades Inteligentes

CDO – Chief Data Officer

COR-Rio - Centro de Operações da Prefeitura do Rio

CPO – Chief Privacy Officer

CRFB - Constituição da República Federativa do Brasil de 1988

DPO – Data Protection Officer

GDPR – General Data Protection Regulation

IBM - International Business Machines Corporation

IoT – Internet of Things

ISO – International Standards Organization

LBS – Location-based Services

LGPD – Lei Geral de Proteção de Dados

NAU – Nova Agenda Urbana

ONU – Organização das Nações Unidas

PbD – Privacy by Design

PET – Privacy Enhancing Technology

RIPD - Relatório de Impacto à Proteção de Dados

RoPA – Record of Processing Activities

SPECTRE – Smart-city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem

TIC – Tecnologia da Informação e Comunicação

“- (...) As cidades, como os sonhos, são construídas por desejos e medos, ainda que o fio condutor de seu discurso seja secreto, que as suas regras sejam absurdas, as suas perspectivas enganosas, e que todas as coisas escondam uma outra coisa.

- Eu não tenho desejos nem medos — declarou o Khan —, e meus sonhos são compostos pela mente ou pelo acaso.

- As cidades também acreditam ser obra da mente ou do acaso, mas nem um nem o outro bastam para sustentar as suas muralhas. De uma cidade, não aproveitamos as suas sete ou setenta e sete maravilhas, mas a resposta que dá às nossas perguntas.”

Diálogo entre Marco Polo e Kublai Khan.

As Cidade Invisíveis, Italo Calvino

1. Introdução

As novas tecnologias da informação e comunicação (TIC) e a chamada quarta revolução industrial estão rapidamente mudando nossas formas de socializar e consumir, influenciando nas mais variadas dimensões da vida humana. A expansão da computação, da comunicação em tempo real, da capacidade de análise de dados em escala massiva e da inteligência artificial possuem efeitos que, de tão recentes, ainda não entendemos com profundidade.

Muito se debate sobre os riscos trazidos por essas tecnologias, como a erosão da privacidade, a difusão de informações falsas, a manipulação de comportamentos, as violações à segurança das informações e as novas formas de vigilância empreendidas tanto por atores privados quanto públicos. A esse processo, movido por uma nova economia baseada na extração de dados pessoais, chama-se capitalismo de vigilância, termo cunhado por Shoshana Zuboff (2021).

Entretanto, a academia ainda se concentra com maior intensidade no ambiente digital, debatendo formas de resistir à vigilância realizada em nossos telefones celulares e computadores. Ocorre que, com a invenção da internet das coisas (IoT), que permite a troca de informações entre os mais variados objetos, fenômenos anteriormente reservados ao ambiente digital transcendem para o espaço físico, o que tende a se intensificar com a chegada da conectividade de quinta geração ou 5G (ECKHOFF, 2018).

A combinação entre a IoT e as novas e potencializadas formas de tratamento de dados, como o processamento de *big data* e o armazenamento em nuvem, produz desafios que representam mais do que a soma dos fatores (AHMED et al., 2014). Isto demanda a atenção da pesquisa neste momento em que essas ferramentas se aplicam ao espaço urbano com o objetivo de criar um modelo urbano, a "cidade inteligente", cuja definição é tema de debate.

O termo *smart city* chama atenção do setor privado e do Estado, que buscam atrair projetos e recursos para a implantação de soluções inovadoras para os problemas urbanos. Soluções tecnológicas influenciam as mais diversas áreas da gestão pública, como o setor de transportes, de fornecimento de energia, de governança e transparência, de habitação, sustentabilidade, entre outros.

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 (MOROZOV; BRIA, 2019). 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 (UNITED NATIONS, 2015).

Contudo, diversas preocupações permeiam a rápida propagação das cidades inteligentes que, diante de especial interesse político-econômico, não são discutidas com a profundidade necessária. Uma crítica ampla às visões dominantes de cidade inteligente não é atrativa para o setor público nem para o setor privado, devendo ser empreendida pela pesquisa e pela sociedade civil. Isto pois a escassez de recurso das administrações municipais e a possibilidade de parcerias milionárias com grandes empresas do ramo multiplica os interesses públicos e privados envolvidos (MOROZOV; BRIA, 2019).

Apesar disso, a forma hegemônica tomada pelos projetos de cidade inteligente contém defeitos em série que se replicam pelo planeta. Denuncia-se, por exemplo, a pouca participação dos cidadãos no debate, a falta de transparência dos projetos, a concentração de partes essenciais da gestão pública na mão de fornecedores privados, os riscos relativos à segurança informacional, a erosão da privacidade dos cidadãos, a possibilidade de aumento da discriminação de grupos vulneráveis e a expansão do controle pelo Estado e pelas empresas.

A dificuldade de promover uma crítica também decorre da flexibilidade semântica do termo "*smart city*" (MOROZOV; BRIA, 2019). Apesar de tratarmos as cidades inteligentes como um objetivo único, não há consenso sobre o que significa a referida "inteligência", já que cada cidade possui necessidades próprias que podem diferir da agenda global. Deste modo, precisamos debater a polissemia das cidades inteligentes para expor a carga política por trás do conceito (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018).

Ao que parece, o processo de disseminação das cidades inteligentes é inevitável. A história demonstra que tecnologias promissoras, assim que descobertas, dificilmente serão largadas ao esquecimento, especialmente quando

são lucrativas para o setor privado e atrativas para o gestor público. Por isso, o presente trabalho rejeita a análise catastrófica ou tecnófoba que vê nas cidades inteligentes uma distopia inevitável. Mais do que uma simples crítica à *smart city* e uma exposição das deficiências, pretende-se a proposição de meios para conciliar o progresso tecnológico com o respeito aos direitos dos cidadãos.

Em suma, este trabalho analisa dois fenômenos contemporâneos que possuem relevância social e acadêmica, mas que ainda não foram abordados em conjunto e de forma aprofundada pela pesquisa brasileira.

Em primeiro, está o citado avanço da agenda de cidades inteligentes, promovida tanto pelo setor público quanto pelo setor privado e sociedade civil, apesar de suas diferentes agendas. Em seu relatório sobre as perspectivas globais de urbanização, a ONU ressalta que que a população urbana deve crescer em 2,5 bilhões até o ano de 2050, afirmando que este processo depende de políticas arrojadas e capazes de garantir a qualidade de vida em cidades cada vez mais cheias (UNITED NATIONS, 2018). A resposta para esses desafios parece vir por meio do conceito de cidade inteligente, o que justifica o estudo de sua relação com outro fenômeno contemporâneo, que é a economia movida a dados pessoais.

O segundo evento é o avanço das leis de proteção de dados pelo mundo, representado especialmente pela publicação, na Europa e no Brasil, do General Data Protection Regulation (GDPR) e da Lei Geral de Proteção de Dados (LGPD). Com o entendimento de que o fluxo cada vez mais intenso de dados pessoais e a capacidade crescente de processamento de dados trazem desafios regulatórios, surge a demanda por um regime legal organizado de proteção de dados. Segundo a ONU, dentre 194 países reconhecidos, 137 já adotaram leis de proteção de dados (UNCTAD, 2021). Tais leis variam em seu escopo e incidência, mas demonstram a necessidade de regulação do tema pelo Estado.

Conectando estes dois pontos, será dedicada especial atenção aos efeitos que a aplicação de TICs às cidades tem sobre a privacidade, a proteção de dados pessoais e a segurança das informações, adotando a premissa de que a proteção de dados é um direito fundamental de especial importância na contemporaneidade. Seguindo a linha preconizada por Stefano Rodotà (2007), a privacidade transcende a proteção do indivíduo, tornando-se questão coletiva de relevância política, social e econômica. Isto é evidente nas cidades inteligentes, em que espaços públicos que

passam a conter, em sua arquitetura, dispositivos que podem se tornar ameaças à privacidade.

No segundo capítulo, serão abordadas as características essenciais para se entender o contexto político das cidades inteligentes no cenário de uma economia movida a dados, fazendo o contraste entre o utopismo propagandeado com a existência de um projeto político-econômico. Neste contexto, será realizada uma breve análise da reação ao urbanismo tecnocrático através do direito à cidade para, ao final, discutir-se o que de fato é uma cidade inteligente, avaliando as definições oferecidas pelos mais variados setores.

Em seguida, o terceiro capítulo pretende estudar os impactos sobre a proteção de dados no ambiente urbano. Para isso, será estudada a evolução do conceito de privacidade, de modo a entender de que forma podemos falar de privacidade em espaços públicos. Serão traçados os pontos de tensão à proteção e dados e à segurança das informações na cidade, para, em sequência, relacioná-los às normas da LGPD. Por fim, será debatida a posição do Poder Público enquanto agente de tratamento de dados e a posição da Carta Brasileira de Cidades Inteligentes como documento de apoio à proteção de dados nas cidades.

Antes de serem tecidas as considerações finais, o quarto capítulo irá abordar, de forma propositiva, as principais formas de mitigar o risco de violação de direitos de privacidade nas cidades inteligentes. Com este objetivo, serão analisados mecanismos jurídicos, organizacionais e tecnológicos que podem viabilizar a criação de cidades inteligentes que tragam melhorias na qualidade de vida sem representar uma ameaça à privacidade. Por fim, este capítulo se encerra com a conclusão de que o direito à cidade deve trazer, em seu conteúdo, o direito à proteção de dados.

Ressalte-se, desde já, que o debate sobre proteção de dados e o estudo das cidades inteligentes podem ser realizados a partir de diversos pontos de partida e a sua combinação comporta resultados variados. Este trabalho não objetiva exaurir os pontos de contato entre os temas, delineando as principais interseções. Ademais, a pesquisa debate temas controversos sem que se pretenda a solução destes, buscando expor de que forma estes assuntos se aplicam ao tema. Quanto às soluções propostas, o trabalho elenca um rol de abordagens que não pretende atingir a solução para um problema tão complexo, mas iluminar caminhos possíveis, que ainda dependem de estudo mais aprofundado.

2. O que é uma cidade inteligente?

Toda pesquisa requer precisa definição sobre seu objeto de estudo. Essa tarefa é um desafio nas ciências humanas, diante da abertura da linguagem e da ambiguidade dos conceitos. Quando falamos sobre algo que possui evidente relevância política e econômica, a definição torna-se mais difícil, surgindo uma disputa discursiva entre a sociedade civil, os setores do mercado e os agentes reguladores. É o que ocorre com as cidades inteligentes no presente. Impactando, ao mesmo tempo, um mercado bilionário e os menores detalhes da vida em sociedade, as *smart cities* são palco de uma intensa luta pelo seu significado.

Desde a primeira menção ao termo nos anos 1990, passando por sua aparição na pesquisa nos anos 2000, 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.

Kitchin, Cardullo e Di Feliciantonio (2018) vinculam o conceito às teorias da justiça, indo além da posição de que as *smart cities* são somente cidades que buscam melhorar a qualidade de vida através da tecnologia. Visões libertárias, por exemplo, poderiam preferir que a relação entre coletores e titulares de dados seja eminentemente privada e regida pela autonomia dos cidadãos. Já a cidade utilitarista seria capaz de adotar tecnologias que, ao custo de certos valores, traria qualidade de vida à maioria. Epistemologias feministas ou antirracistas, por sua vez, buscariam formas de adaptar a cidade às demandas por igualdade.

Evidentemente, nenhum conceito é tão simples como nos exemplos acima. Mas é possível encontrar posicionamentos que nos lembram que a definição da arquitetura de uma cidade é questão política. É comum ouvir, por exemplo, que o aumento da vigilância nas cidades se justifica diante da promoção da segurança, refletindo o posicionamento utilitarista (FIRMINO, 2018). Também se justificam controversas formas de tratamento de dados a partir da visão libertária de que os

cidadãos possuem a autonomia de se opor às tecnologias que os rodeiam, a partir da negativa de consentimento.

Logo, o uso de novas tecnologias é uma questão social relevante, tendo efeito sobre a convivência humana, as eleições, o consumo e o exercício do poder. Não há por que esperarmos que sua aplicação nas cidades será diferente, especialmente diante do crescimento dessas. Entre 1950 e 2018, a população urbana passou de 750 milhões para 4,2 bilhões, havendo a expectativa de que, até 2050, 70% dos humanos viverão em cidades (UNITED NATIONS, 2018).

Então, é natural que a definição sobre como a tecnologia será aplicada no espaço urbano e sobre quais são as prioridades de uma cidade são questões políticas, especialmente diante do fato de que a urbanização contemporânea é muito mais rápida em países pobres e desiguais[1]. Ainda assim, o debate sobre a definição de cidade inteligente é dominado por discursos que adotam uma visão despolitizante, tratando a cidade inteligente como um modelo ótimo, único e aplicável a contextos urbanos distintos (MOROZOV; BRIA, 2019). Isto contribui para a estagnação do debate e das propostas alternativas de cidade, que podem ajudar a mitigar os efeitos negativos sobre os direitos fundamentais dos cidadãos.

Neste capítulo, abordaremos questões fundamentais sobre a economia contemporânea, dependente de tratamento de dados pessoais em larga escala. Em seguida, será detalhada a construção do discurso hegemônico sobre as cidades inteligentes. Além do elemento discursivo, debateremos como o legado do urbanismo moderno se relaciona com as cidades inteligentes, impondo uma espécie de urbanismo tecnocrático e desenhado de baixo para cima, com pouco espaço para participação popular. Por fim, serão trazidos conceitos de cidade inteligente, concluindo com a adoção de uma definição funcional que permite a análise prática dos efeitos sobre a privacidade e proteção de dados pessoais.

2.1. As cidades e a economia movida a dados pessoais

Falar em progresso tecnológico na segunda década do século XXI é contar a história de como os dados pessoais tornaram-se o elemento central da economia e da política global. Não à toa, surgem em termos como *data driven economy*, ou

[1] Até 2050, 90% do crescimento populacional urbano se dará na Ásia e na África (UNITED NATIONS, 2018).

seja, economia movida a dados pessoais, marcando uma transição causada pelo surgimento de novas tecnologias de extração e análise de dados (FRAZÃO, 2020).

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 e processadores dobra a cada dois anos (MOORE, 1998). Tal aceleração permite o aumento de potência e a redução no preço de computadores, possibilitando o surgimento de imensos bancos de dados que podem ser analisados de forma rápida e precisa. Dessa forma, surgem termos como *big data*, computação em nuvem e outras técnicas de uso de dados pessoais em escalas antes inimagináveis, tornando-os insumos para a maioria das decisões políticas e econômicas do futuro.

Esses fatores contribuem para o entendimento de que estamos diante da quarta revolução industrial, que se distingue das anteriores por seu crescimento exponencial e não linear. 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 permitem que os atores públicos e privados obtenham informações em escala inédita sobre os cidadãos, agravando a assimetria informacional entre as pessoas e as corporações e o Estado. O acúmulo de informação representa um ativo econômico valioso, já que o conhecimento sobre os hábitos das pessoas permite que estes sejam utilizados e até mesmo influenciados pelo mercado.

Este modelo de negócios acabou por tornar a extração de dados pessoais uma atividade econômica baseada na vigilância sobre nossas vidas, registrando nossos hábitos, deslocamentos, padrões de consumo e tudo que for possível extrair, armazenar e analisar. A este sistema econômico Zuboff deu o nome de capitalismo de vigilância, uma "*nova forma de capitalismo da informação que procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado*" (2018, p. 18). Os dados sobre o comportamento humano tornam-se matéria prima de uma nova lógica de acumulação baseada na premissa de que nenhuma informação é irrelevante, já que podem ser utilizadas para a previsão de comportamentos e tendências futuras.

Como explica Zuboff (2021), o ciclo da vigilância se inicia com dados coletados a partir da difusão praticamente ubíqua de tecnologias capazes de receber e enviar dados pessoais. Estes dados são, então, extraídos de forma vertical, sem consentimento e com pouca supervisão pelo Estado. Após a extração, esses dados são analisados a custos baixíssimos, dando origem a dados secundários capazes de gerar receita através da venda ou da sua utilização para fins econômicos diretos. Dessa maneira, a extração de dados é interessante para todos os atores, pois, mesmo que estes dados sejam inúteis para quem os extrai, eles podem ser compartilhados com os setores interessados em comprá-los.

Os atores deste sistema se sustentam a partir de uma redistribuição dos direitos de privacidade (ZUBOFF, 2018), já que reduzem a privacidade do indivíduo enquanto mantêm suas práticas resguardadas pelo sigilo comercial e industrial. Enquanto os novos poderes buscam conhecer os indivíduos em seus mínimos detalhes, o seu funcionamento é obscuro e regido por algoritmos pouco conhecidos pela sociedade, conforme exposto na célebre *black-box society* de Frank Pasquale (2015). Tal assimetria de poder e conhecimento permite que esse processo se divulgue como progressista e benéfico, utilizando narrativas como a criação de um ideal "*smart*" em que toda inovação representa um avanço da sociedade, sendo a troca da privacidade por benefícios gratuitos uma troca justa.

É neste contexto, da expansão da tecnologia sobre a vida humana e de discursos que buscam despolitizar a tecnologia, que se insere a narrativa dominante sobre as cidades inteligentes. O espaço urbano, com a possibilidade de introdução das novas tecnologias, torna-se um terreno a ser desbravado pela economia movida a dados.

Entretanto, não se pretende negar que estas tecnologias podem ser utilizadas para potencializar a produtividade, a segurança e a qualidade de vida nas cidades. Em muitas ocasiões, isto de fato ocorre, existindo bons exemplos pelo mundo. Ademais, as cidades inteligentes são uma necessidade contemporânea, haja vista o intenso crescimento populacional e a presença de desafios que requerem abordagens sofisticadas, como a violência, as mudanças climáticas e os crescentes desastres ambientais (HILLER; BLANKE, 2017).

A utilização da tecnologia para a abordagem desses problemas é positiva, sendo inclusive parte da Nova Agenda Urbana (NAU) definida pela ONU-Habitat em 2016 (REIA, 2019). Porém, munidos de uma análise crítica, somos capazes de

entender quais lógicas estão em jogo e que as cidades inteligentes podem replicar a lógica da vigilância e da violação à privacidade. Em tal cenário, qualquer benefício social advindo da aplicação das tecnologias será colhido em um ambiente urbano moldado para o mapeamento e modificação de comportamentos humanos, em um perigoso cálculo utilitarista que pode ser evitado.

Esta análise torna-se ainda mais relevante pois a moldagem do espaço urbano é entendida como forma tradicional de exercício do poder[2], como demonstra o estudo de Foucault sobre o processo de racionalização do poder ou de *governamentalidade,* através do qual o Estado deixa de ser um mero impositor de leis e passa a exercer o poder com finalidades cientificamente definidas. Em sua obra "Segurança, Território e População" (2008), o autor expõe como o modelo de cidade se altera de acordo com a lógica de poder existente, demonstrando a transição a partir de três projetos urbanos.

Em primeiro, o Estado buscou garantir a sua soberania a partir da definição de seus limites jurídicos e da garantia de uma capital ao centro. Protegida das ameaças externas, a cidade passa a necessitar de mecanismos para disciplinar seus habitantes, especialmente diante do êxodo rural decorrente da revolução industrial. Surgem a polícia, a cadeia, a escola, os hospitais e outras instituições que buscavam inserir os cidadãos em uma nova lógica produtiva.

Em seguida, essas cidades tornam-se superlotadas e as doenças se proliferam, o que passa a ser abordado a partir de novas técnicas, como estudos estatísticos e probabilísticos, culminando na visão de que a cidade deve ser desenvolvida com base em dados (ALVES, 2019). O Estado racionalizado passa a poder influenciar nas condições de vida do corpo social e a agir em nível de macropoder, abordando a população inteira em conjunto como o objeto de uma atuação baseada em cálculos (LEMKE, 2011). Como se vê, o uso de dados e a alteração do espaço urbano através uma abordagem racionalista fundada em dados

[2] Richard Sennet, da perspectiva de um urbanista, também correlaciona as formas hegemônicas de constituição da malha urbana com o exercício do poder. Leia-se: "A malha urbana se manifesta de três formas. A primeira é a grelha ortogonal, como a que dava forma às antigas cidades romanas. (...) O segundo tipo de malha surge quando são unidos pátios, criando uma cidade celular (...). O terceiro tipo de malha é a grelha constitutiva. Foi este o plano de Cerdà para Barcelona. (...). Cada um desses tipos de grelha define determinado espaço de poder, ou de resistência ao poder. A grelha divisível representava a dominação romana, irradiando-se do centro o poder político, que se reproduzia em cada espaço subdividido. A grelha celular com frequência tem servido de espaço secreto para habitantes destituídos de poder, um espaço de difícil penetração para as autoridades (...). A grelha constitutiva tem servido na era moderna como ferramenta do poder capitalista." (SENNET, 2021, p. 53)

pessoais não é uma característica inédita das cidades inteligentes, mas uma consequência da racionalização do poder estatal.

Hoje, 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 tipo 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).

E, em um cenário de assimetria informacional entre cidadãos, empresas e Estado, o exercício do poder sobre o espaço urbano nas cidades inteligentes é difícil de se questionar, sendo levado a cabo a partir de mecanismos ainda pouco conhecidos pela população e que se pretendem despolitizados. Segundo o discurso propagandeado, não se trata de utilizar dados para fins políticos ou econômicos, mas da obtenção da "verdade real" através de dados, usados para a solução técnica dos problemas urbanos, em um caminho de superação das cidades ultrapassadas (MOROZOV; BRIA, 2019).

Contudo, trata-se de uma narrativa distante da realidade:

> Algumas inquietações surgem quanto ao perigo que esse "sonho" da cidade inteligente, governada por algoritmos, apresenta para a nossa liberdade. Quanto mais informações nós disponibilizamos, mais nos tornamos transparentes para os algoritmos que "facilitam" a nossa vida, mais nos tornamos conhecidos em nossos mínimos detalhes, e cada vez mais os algoritmos serão capazes de antecipar nossas condutas, oferecer serviços e direcionar nossas ações. Mas é um equívoco acreditar que os algoritmos simplesmente oferecem aquilo que queremos. Mais do que isso, eles fazem com que algo seja desejável (ALVES, 2019, p. 31)

Ademais, experiências locais demonstram que parte dos programas de cidades inteligentes pode ter semelhanças com o chamado novo urbanismo militar, priorizando aplicações tecnológicas voltadas para a securitização de espaços e para estratégias de segurança pública. Stephen Graham (2011) argumenta que, após o atentado do 11 de setembro de 2001, se inicia um processo de disciplinarização dos espaços urbanos através da reutilização de tecnologias criadas para finalidades militares, como *drones* e câmeras dotadas de inteligência artificial. O valor da

"segurança nacional", então, foi um relevante propulsor da inclusão de mecanismos de vigilância tecnológica no tecido urbano.

O Brasil e, mais especificamente, o Rio de Janeiro, foram espaços de experimentação do novo urbanismo militar. Em razão dos megaeventos como a Copa do Mundo e as Olimpíadas, as cidades foram tratadas como laboratórios para empresas de tecnologia e de segurança e atraíram a atenção para a criação de infraestruturas centralizadas de comando e controle (CARDOSO, 2018). Assim, o Rio de Janeiro inaugurou o Centro de Operações Rio (COR-Rio), em parceria com a empresa IBM, para monitorar questões como o tráfego, as condições climáticas, as mídias sociais e alertas ambientais. Estes centros aparecem como "*característica de um modelo de cidade inteligente centralizador e eficiente*" (FIRMINO, 2018, p. 73), mas trazem riscos de vigilância exacerbada e militarização do cotidiano.

Ainda assim, a inserção das cidades inteligentes na lógica da economia movida a dados, do capitalismo de vigilância e do novo urbanismo militar não é um processo inevitável rumo a um cenário distópico. A aplicação destes mecanismos pode ser acompanhada de ganhos de qualidade de vida e a sociedade está cada vez mais equipada para entender que o excesso de vigilância pode ser problemático. É o que se vê através do avanço de leis nacionais de proteção de dados pessoais e da criação de órgãos fiscalizadores locais. Posteriormente, serão abordadas formas práticas para que seja possível a conciliação entre os benefícios das cidades inteligentes e os direitos de privacidade e proteção de dados.

Neste cenário, cabe à sociedade civil e aos pesquisadores o questionamento sobre a necessidade do uso de tecnologia e do processamento de dados pessoais para cada finalidade específica, avaliando a adequação de cada projeto de cidade inteligente às prioridades locais (DONEDA; MACHADO, 2019). Entendidos como mecanismos que podem exacerbar a vigilância, estes devem ser adotados quando representarem um ganho significativo de qualidade de vida e tiverem conexão com os problemas locais. E isto somente é possível a partir do entendimento da narrativa criada em torno das cidades inteligentes.

2.2. Entre a narrativa e a política das cidades inteligentes

É natural que a transformação do espaço urbano seja perene foco de interesses políticos e econômicos ao longo da história. Entretanto, por dois fatores

recentes, as oportunidades econômicas advindas do planejamento de cidades atingiram níveis inéditos, explicando a necessidade de construção de uma estratégia discursiva capaz de difundir um modelo unificado e lucrativo de cidades inteligentes a ser replicado de forma universal.

Em primeiro, destaca-se o expressivo crescimento demográfico nas cidades. Em tal cenário, surgem duas oportunidades: grandes mercados consumidores para as soluções tecnológicas e a necessidade de reorganizar as cidades para receber contingentes cada vez maiores de pessoas, demandando estratégias para organizar desafios complexos, como o trânsito, a poluição, a violência e o consumo de energia. Os problemas urbanos tornam-se ainda mais graves em um contexto de aquecimento global e mudanças climáticas, o que exige o controle da sustentabilidade pelos governos locais. Assim, cidades passam a demandar soluções complexas, específicas e dependentes de um *know-how* especializado que dificilmente poderá ser provido pelo poder local (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018).

Governos municipais passam a buscar parceiros privados para empreender soluções técnicas, atrair investimentos e reduzir os gastos públicos. Diante da promoção de políticas de austeridade fiscal, o setor público torna-se cada vez menos um gestor direto e mais um consumidor de soluções prontas de especialistas privados. Ainda, a busca por investimentos e mão de obra especializada reforça a necessidade de criação de uma marca de cidade inteligente e inovadora, tornando o uso de tecnologia uma espécie de selo de qualidade para cidades, sendo possível ranquear cidades de acordo com seu índice de *smartness* (WOETZEL et al., 2018).

Em segundo, no século XXI começam a surgir novas formas de influenciar a cidade a partir das TICs (ECKHOFF; WAGNER, 2018). A criação da informática em geral já havia revolucionado a gestão pública diante da potencializada capacidade de processamento de dados e de comunicação. Porém, o avanço da tecnologia permite a interação, em tempo real, entre os cidadãos e a cidade. Tornou-se possível, por exemplo, coletar, armazenar e analisar dados captados por sensores alocados nos mais variados objetos, como carros, postes de luz, câmeras de trânsito e latas de lixo, permitindo a criação de sistemas específicos para a gestão do tráfego, do consumo de energia ou da emissão de poluentes (MAGRANI, 2018).

A evolução do processamento de dados também viabiliza a criação de estatísticas e a geração de informações úteis para a melhoria da transparência e

eficiência da administração pública, que adota novos mecanismos para a interação com a população. E, logicamente, para todas essas novas demandas, existem novas ofertas, quase todas surgidas no setor privado, mais capaz do que o Estado para acompanhar e ditar o ritmo da inovação.

É diante desses dois fatores que se cria um discurso capaz de difundir ao máximo as novas tecnologias para este gigante mercado. Isto significa que, como ocorre na maioria das campanhas publicitárias, demandas urbanas já existentes serão somadas a um discurso que também objetiva criar demandas onde elas ainda não existem. Para isso, propagam-se produtos e soluções aparentemente universais, mas que nem sempre se adaptarão às realidades locais (ISMAGILOVA et al., 2020).

O primeiro passo foi a adoção do termo "*smart*", que se torna uma marca distintiva, mas que possui uma variedade de significados possíveis. O *smart* passa a ser considerado símbolo de irreverência, avanço e disrupção, trazendo uma evolução contínua rumo ao futuro. As cidades que não forem capazes de se adaptar ao ideal, argumenta-se, se tornarão incapazes de solucionar seus problemas, de captar recursos e atrair cidadãos qualificados (MOROZOV; BRIA, 2019). E, mesmo com pouca clareza sobre o que é *smart*, aceitamos que nossos telefones celulares, relógios e até nossas cidades precisam ser inteligentes.

A propagação deste discurso tem origem no programa "*Smarter Cities*", patenteado pela 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. Naturalmente, aquele que cria a narrativa assume uma posição de poder, podendo atribuir significados aos termos.

É essa a posição que, em geral, o setor privado assume: serão as empresas de tecnologia que inicialmente definem o tipo de "inteligência" que será adotado nas cidades pelo mundo. 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 (OPP – *obligatory passage points*) 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, tornando as cidades dependentes de seus produtos. Este processo de divulgação tem fundamento na chamada teoria do ator-rede[3] (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 (SÖDERSTROM et al., 2014).

O mecanismo utilizado para a difusão da narrativa de cidades inteligentes, tornando-a universal e apolítica, se baseia na teoria dos sistemas, cuja tradição organicista remonta ao século XVII e a autores como William Harvey, que comparava a cidade com um organismo vivo dotado de sistema circulatório (SÖDERSTROM et al., 2014). Na contemporaneidade, a metáfora do corpo humano substitui-se pela cidade-computador, composta por sistemas divisíveis e replicáveis em todo lugar. A cidade-computador possui redes interconectadas, que são interpretadas por uma matriz centralizada e capaz de correlacionar as informações em busca de soluções (SENNET, 2021).

Assim, ao exemplo da pioneira IBM, a cidade é dividida em três pilares centrais (planejamento e gestão, infraestrutura e recursos humanos), cada um divisível em mais três pilares, totalizando nove dimensões (segurança, edifícios, planejamento urbano, governança, administração, energia, água, meio-ambiente e transporte). Para cada uma dessas dimensões, o setor privado possui soluções inteligentes, enquanto a soma dessas nove dimensões constitui uma cidade mensurável a partir de centros de operação, a exemplo do citado COR-Rio, criado no Rio de Janeiro em parceria com a própria IBM (FIRMINO, 2018).

A cidade é, então, um sistema composto por menores sistemas. A teoria dos sistemas urbanos cria uma relação de equivalência entre as cidades, usando uma linguagem capaz de traduzir fenômenos urbanos variados através de combinação e análise de dados. As cidades deixam de ser criadas pela sua realidade social, mas sim pelos dados obtidos a partir destes processos sistêmicos. O entendimento dos problemas urbanos não demanda mais especialistas, bastando a mineração e análise

[3] A teoria do ator-rede foi elaborada pelo pensador francês Bruno Latour (2000). O autor rejeita o pensamento que analisa os seus objetos de forma estática, privilegiando o posicionamento destes com relação àquilo que já existe e o que está sendo construído. Em vez de realizar a análise de um fenômeno somente de acordo com o que já está estabelecido, Latour defende que se estude o fenômeno em seu processo de construção. Dessa forma, todos os conceitos atuam como nós em uma rede, possuindo, além de um conteúdo próprio, formas que surgem em razão da relação entre estes nós.

de dados obtidos através das TICs, em uma postura positivista que desvaloriza o contexto histórico, político e científico do local em que incide (SÖDERSTROM et al., 2014).

Tal discurso, se adotado de forma descuidada, pode ser tecnocrático, criando uma moldura na qual problemas urbanos não são questões políticas, mas técnicas. Essa busca por neutralidade política é uma característica da teoria de sistemas, cujo funcionamento não é conservador nem progressista, sendo somente a decomposição de um fenômeno em partes relacionáveis (SÖDERSTROM et al., 2014). Não à toa, as mesmas práticas de cidades inteligentes são a ordem do dia em países com problemas, culturas, sistemas políticos e cidades radicalmente diferentes, como a China e os Estados Unidos da América (OAV, 2019).

Porém, apesar do discurso, a alocação de recursos decorre de decisões decorrentes da disputa entre poderes, da escolha de prioridades, do *lobby* de setores relevantes, entre outros fatores claramente politizados. Transformar uma cidade em *smart city* significa realizar a escolha política de priorizar o investimento em tecnologia privada (KITCHIN, 2015). E, nos mais variados lugares, as empresas que divulgam os produtos utilizados são pontos de passagem obrigatórios, já que fornecem as soluções capazes de abordar os problemas na forma em que estes são desenhados, ou seja, com base na teoria de sistemas.

Isso não significa que a opção por adotar uma visão baseada em sistemas seja uma escolha essencialmente equivocada que merece ser descartada. Mas é preciso ter atenção ao discurso que considera as cidades devem seguir o mesmo rumo através das mesmas tecnologias. Tal alerta torna-se especialmente urgente em cidades que sofrem com problemas prioritários, como a falta de moradia digna ou saneamento básico, que devem ter a oportunidade de decidir se o investimento em tecnologia é mais urgente que questões que afetam direitos básicos dos seus cidadãos.

A esta forma contemporânea de resolução de problemas, dá-se o nome de solucionismo (MOROZOV, 2018), que consiste na inversão do fluxo de construção de soluções coletivas e conectadas às demandas sociais dos cidadãos urbanos[4]. Em

[4] Richard Sennet (2021, p. 188) afirma: "A cidade inteligente prescritiva privilegia a solução de problemas em detrimento da detecção de problemas. Na boa ciência, o pesquisador quer conhecer os efeitos colaterais de uma nova droga; na boa carpintaria, o profissional procura prever os problemas que surgirão ao envernizar um armário, depois de descobrir como juntar duas madeiras de texturas diferentes. A solução de problemas e a detecção de problemas estão ligadas – desde que

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). A utilização de soluções pré-fabricadas e universais nem sempre irá se amoldar às prioridades das cidades, podendo, a custos elevados, não ter impacto significativo na qualidade de vida dos cidadãos.

Como se vê, políticas de *smart cities* envolvem a gestão de recursos públicos e a adoção de tecnologias que terão impacto no cotidiano e na qualidade de vida dos cidadãos. São questões que envolvem o núcleo duro da atividade política, apesar da utilização de discurso tecnicista e despolitizante (MOROZOV; BRIA, 2019). Tal estratégia não é algo a ser abordado com desespero, já que é propagada por atores privados em um sistema econômico capitalista, que naturalmente objetivam a máxima difusão de seus produtos.

Contudo, é necessário entender que a visão fundada na teoria de sistemas e no solucionismo é uma estratégia de mercado, que, além dos benefícios prometidos, também pode vir a causar prejuízos à sociedade. Não se trata de recorrer à tecnofobia ou de afirmar que as soluções apresentadas são essencialmente inadequadas, mas de adotar uma postura cética quanto ao teor dos discursos. Descortinando o que há de narrativa e o que há de verdadeiro, é possível entender quais soluções melhor se amoldam a cada realidade e descartar a visão que universaliza e simplifica a cidade inteligente.

2.3. Do urbanismo progressista ao direito à cidade (inteligente)

A existência de uma abordagem urbanística racional baseada nas mais avançadas tecnologias da época precede o fenômeno das *smart cities* em milênios. Ao menos desde o mundo antigo, busca-se a orientação da cidade de acordo com a "inteligência" disponível, seja para impor um modelo de habitação ou para decidir, de forma comunitária, como construir a cidade. Não à toa, a história nos traz exemplos de cidades que foram mais ou menos inteligentes, em sentido amplo, na organização do espaço.

---

seja curioso. Mas o modelo prescritivo embota a curiosidade; nesse tipo de cidade inteligente, não é necessário sê-lo".

Segundo Jean-Louis Harouel (2004), historiador do urbanismo, Platão e Aristóteles escreveram extensas contribuições para a construção das cidades gregas, reclamando uma separação do terreno a partir das funções que cada local deve desempenhar. Haveria, então, o espaço reservado para a política (ágora) e locais para a realização de atividades comerciais, buscando a separação entre o econômico e o político. Como se vê, a cidade grega era esquematizada para permitir o exercício da vida comum local, tendo as diretrizes definidas a partir das decisões tomadas democraticamente.

Também em Roma vemos outra característica das cidades inteligentes: a criação de um tipo ideal de cidade a ser replicado pelo mundo (SENNET, 2021). O Império Romano, de natureza conquistadora, se espalhou até a África e a Ásia, criando cidades cuja identidade originava de um plano urbanístico comum. O urbanismo romano era baseado em um traçado ortogonal cortado na vertical e na horizontal por duas vias que criavam quatro quadrantes nos quais se distribuíam o *fórum*, os órgãos da administração pública e as habitações. Eram elaborações fundadas com base em legislação urbanística e executadas servidores públicos com competências previamente definidas (HAROUEL, 2004).

Logo, a existência de um urbanismo inteligente, em sentido amplo, não é fenômeno recente. As cidades inteligentes contemporâneas replicam características de diversos períodos históricos, dentre os quais se destacam o utopismo e o chamado urbanismo progressista em suas diversas fases. Harouel entende que utopistas abordam a cidade de forma impositiva, moldando-a com objetivos previamente definidos, rumo à cidade ideal. O utopismo, apesar de seu verniz redentor, se esteia em "*sistemas constrangedores e repressivos que se escondem atrás de fórmulas agradáveis*" (HAROUEL, 2004, p. 113).

O urbanismo utopista adota uma visão de "cidade doente", para posteriormente oferecer um discurso baseado em soluções terapêuticas universalistas, que podem ser aplicadas em qualquer realidade local. No caso da cidade inteligente, o espaço urbano é descrito como violento, poluído, administrado por um Estado ineficiente e obsoleto (RENNÓ et al., 2016), ao qual se contrapõe a cidade inteligente, sustentável e transparente. Assim como nas maquetes e esquemas de utopistas como Thomas Morus e Fourier, a *smart city* é apresentada como um plano integrado, de funcionamento ideal e globalmente replicável. Contudo, em vez de um utopismo fundado na conformação do espaço, o "utopismo

inteligente" oferece soluções terapêuticas baseadas no processamento de dados (SÖDERSTROM et al., 2014).

Estes sonhos utopistas são alimentados pela vertente tecnocrática que se origina a partir do urbanismo progressista do século XIX, personificado pelo Barão de Haussmann, responsável pela reforma de Paris a partir de um planejamento racional-tecnicista (BARBOSA; COSTA; PONTES, 2020). Assim como a *smart city*, as cidades do auge do capitalismo industrial novecentista são criadas por uma classe de técnicos que se distancia dos setores populares e impõe reformas radicais que emanam do centro para a periferia.

Como no presente, a cidade haussmaniana buscava atrair um tipo ideal de homem, que era pensado de forma única e que tinha as suas necessidades supridas pela cidade moderna. Deste modo, o centro das cidades precisa ser higienizado, as vias precisam ser expandidas, demolem-se cortiços e criam-se parques públicos para reduzir a poluição (SENNET, 2021). O mesmo processo pode ser verificado nas reformas do "bota abaixo" de Pereira Passos que, às custas de repetidas violações de direitos, recriou o centro do Rio de Janeiro, então capital do Brasil, aos moldes da Paris de Haussmann.

Da mesma forma que a narrativa da *smart city*, o urbanismo progressista se pretende uma ciência global da cidade que pode ser aplicada em qualquer lugar, como bem manifestam os princípios do urbanismo moderno influenciado, no século XX, pelo pensamento de Le Corbusier. Tal forma de pensar, como a cidade inteligente, foi influenciada invenções de então, como a indústria, o automóvel e o avião. Essa ideologia representava um universalismo aplicável tanto às pessoas quanto ao espaço, silenciando as formas de vida e de convivência que não se adaptassem ao discurso dominante. Como expõe Harouel (2004, p. 121):

> O esquema urbano é considerado válido para qualquer lugar pois ele é concebido para o homem-padrão. Para Le Corbusier: 'todos homens possuem as mesmas necessidades'. Assim, os urbanistas progressistas retomam as mesmas soluções no mundo inteiro, tanto para as grandes quanto para as pequenas cidades.

Os paralelos com a narrativa das cidades inteligentes são evidentes. Assim como as cidades pensadas na era de ouro do capitalismo industrial, as *smart cities* buscam atrair uma espécie de tipo ideal de homem: jovem, qualificado, conectado e inovador. Também objetivam a atração de recursos privados, o estabelecimento de sedes negociais de grandes empresas de tecnologia e a criação de bairros e

distritos pensados especificamente para as necessidades deste tipo de cidadão e deste modelo econômico (GRAHAM, 2011).

Sennet (2021) afirma que as ideias que originaram cidades inteligentes derivam de duas fontes: o Plan Voisin e a Carta de Atenas. O primeiro, elaborado por Le Corbusier, defendia o urbanismo puramente funcional, desejando que a cidade pudesse funcionar como uma espécie de máquina, com ruas amplas permeadas por séries de conjuntos habitacionais. Já a Carta de Atenas foi elaborada por especialistas em 1933 com o objetivo de encontrar o modelo funcional que deveria orientar o urbanismo no século XX, a partir da síntese entre quatro fatores: vida, trabalho, lazer e circulação.

Sennet afirma que: "*O plano e a carta presidem uma versão de 'cidade inteligente', na qual a alta tecnologia tenta reduzir as confusões inerentes à vida num lugar complexo*" (2021, p. 94). Enquanto Le Corbusier e seus contemporâneos objetivavam vincular toda forma urbana a uma função, a cidade inteligente aparentemente repete o mesmo objetivo. Leia-se:

> (...) Lewis Mumford, advertia para os riscos da tecnologia desalmada ao estilo de Le Corbusier; ainda assim, sua versão da cidade inteligente também era um lugar em que forma e função se fundiam de maneira perfeitamente mecânica – tudo tem seu lugar e sua lógica, todos os elementos do viver são estabelecidos com precisão no estrito traçado radial. As cidades inteligentes de hoje trazem a coadunação forma-função para a era digital, com o objetivo de gerar ambientes autossustentáveis. Uma adequação muito rígida entre forma e função é a receita certa de uma obsolescência tecnológica. (SENNET, 2021, p. 186)

Desse modo, apesar da maior possibilidade de participação popular que nos projetos dos séculos passados, as cidades inteligentes relembram o urbanismo modernista em sua dependência de uma classe técnica responsável pela imposição de um modelo científico. Tal urbanismo "*top-down*" (FINCH; TENE, 2016), ou seja, criado de cima para baixo, é executado de acordo com as necessidades do cidadão e da cidade ideais, modelos universalistas muitas vezes distantes das demandas mais urgentes e dos cidadãos desprivilegiados.

A cidade de Songdo, na Coreia do Sul, é citada como um exemplo de cidade planejada de cima para baixo, sem participação popular. Trata-se de um experimento realizado através de uma parceria entre a prefeitura local e empresas de telecomunicações, como a Cisco, com o objetivo de criar um distrito capaz de funcionar com base no processamento de dados coletados. Songdo é criticada por

sua grave dependência com relação à empresa, que possui contratos para garantir a exclusividade com relação aos sistemas providos, tornando-se um ponto de passagem obrigatório para as soluções na cidade (SENNET, 2021).

Mas existem exemplos de participação cidadã, demonstrando que é possível a construção de cidades inteligentes "de baixo para cima" (*bottom-up)*. É o caso de Barcelona, que aposta em processos colaborativos, guiando-se através do princípio de *city data commons* (dados da cidade abertos) com a intenção de, ao mesmo tempo, se beneficiar do uso de dados e garantir a soberania digital[5] da população. Trata-se de uma estratégia de inovação ancorada na autodeterminação informativa dos cidadãos e na transparência dos processos de implementação de novas tecnologias (MOROZOV; BRIA, 2019).

A inclusão do cidadão e das necessidades da população em primeiro plano é um dos pilares do direito à cidade, construção teórica de Henri Lefebvre (2001) que surge como reação às imposições do urbanismo modernista e da visão universalista de cidade unicamente voltada para a produção capitalista. Nas cidades inteligentes, o direito à cidade reassume seu protagonismo como ferramenta que pode iluminar o caminho a ser seguido para que se atinja o objetivo de uma cidade inteligente verdadeiramente democrática.

O direito à cidade é, hoje em dia, o principal vetor da Nova Agenda Urbana defendida na Conferência Habitat III das Nações Unidas, que dedicou uma de suas 22 sessões para discussão das cidades inteligentes (UNITED NATIONS, 2016). A ONU parte do pressuposto de que as formas vigentes de urbanização não foram capazes de combater a desigualdade e a exclusão, pensando o direito à cidade como um enquadramento que permite pensarmos a cidade em uma ótica fundada nos direitos do cidadão. Dessa forma, a organização entende o direito à cidade como o "*direito de todos os habitantes, atuais e futuros, de ocupar, usar e produzir cidades justas, inclusivas e sustentáveis, definidas como um bem comum essencial para a qualidade de vida*" (REIA, 2019, p. 156), defendendo que as soluções tecnológicas devem ser abordadas tendo a igualdade e a inclusão social como prioridades.

Especialistas no "direito à cidade inteligente" (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018) afirmam que a maioria das *smart cities* é pensada com

[5] "Technological sovereignty is the notion that technology should be orientated to and serve local residents, and be owned as a commons, rather than applying a universal, market-orientated, proprietary technology" (KITCHIN, 2018).

base nos interesses de uma minoria ligada ao seu planejamento, uma elite empreendedora capaz de interagir com as soluções implementadas. É somente após o estabelecimento dos objetivos e das diretrizes de implementação que ocorre o engajamento com a comunidade local, que possui pouca força para reorientar o projeto já definido. Apesar do discurso que divulga os projetos como focados nas necessidades do cidadão, a verdade é que o direito de poder moldar o espaço de acordo com a vontade cidadã está distante das cidades inteligentes.

Mais do que habitar e ocupar a cidade, as pessoas devem ter o direito de participar da cidade, ou seja, de determinar como será organizado o espaço urbano de acordo com as necessidades reais da população. Trata-se de uma demanda ancorada na dignidade da pessoa humana, se estendendo por direitos como a igualdade, a informação, a livre expressão e a participação política (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018). Os citados direitos tem especial relevância em um cenário de assimetria informacional, no qual os cidadãos se encontram alijados do entendimento completo sobre os processos em curso e despidos do conhecimento necessário para influir na construção da cidade.

Em conclusão, diante de um movimento tecnocrático que parece reviver as utopias do urbanismo modernista, é possível ver no direito à cidade uma forma de politizar a cidade inteligente (BARBOSA; COSTA; PONTES, 2020). De tal modo, torna-se possível o questionamento amplo e comunitário sobre de que forma a cidade pode ser um projeto ancorado nos direitos do cidadão, respeitando o seu direito de participar da cidade, a sua soberania tecnológica e sua autodeterminação informativa. No quarto capítulo, o direito à cidade será explorado de forma mais aprofundada, de modo a incluir o direito à proteção de dados como parte essencial de sua composição.

2.4. A busca por uma definição de ‘cidade inteligente’

Precisamos concretizar o direito à cidade para que o modelo de cidade inteligente não reproduza lógicas de vigilância e aumento da desigualdade. Entretanto, para que possamos defender um modelo inclusivo de cidade inteligente, é necessário entender o que o termo significa. Conforme argumentado, o termo *smart*, comumente traduzido como inteligente, é polissêmico. Porém, um ponto comum sobre as definições de cidade inteligente decorre da aplicação de tecnologia

com a finalidade de melhoria da qualidade de vida no ambiente urbano (GALATI, 2018).

Porém, ao desenvolver-se uma definição mais completa, os conceitos refletem objetivos distintos, podendo priorizar o 'fator tecnologia' ou o 'fator qualidade de vida'. Fornecedores privados de tecnologias costumam oferecer definições de cidade inteligente conectadas aos produtos oferecidos, como vimos a partir da definição baseada na teoria dos sistemas fornecida pela IBM. A empresa conceitua a *smart city* como a cidade que utiliza a informação e a tecnologia para captar, analisar e integrar dados dos principais sistemas de uma cidade (DIRKS; KEELING, 2009). A postura adotada pela Cisco (2022), líder global na venda de dispositivos dotados de IoT, é semelhante:

> Uma cidade inteligente usa a tecnologia digital para conectar, proteger e melhorar a vida dos cidadãos. Sensores de IoT, câmeras de vídeo, redes sociais e outros dispositivos agem como um sistema nervoso, fornecendo ao operador da cidade e aos cidadãos um *feedback* constante para que possam tomar decisões informadas.[6]

As definições utilizadas pelo setor privado trazem a empresa emissora do conceito como ponto de passagem obrigatório, fornecendo definições baseadas em tecnologias que estas são capazes de oferecer. Essas conceituações costumam ser oferecidas em panfletos acompanhados das diversas soluções vendidas pelas empresas, demonstrando como o modelo de cidade descrito pode ser atendido pelas tecnologias disponíveis.

Para ilustrar o que é a cidade inteligente do presente, cabe trazer breves exemplos de aplicações concretas. É o caso, por exemplo, da adoção de câmeras dotadas de reconhecimento facial para prevenção de crimes, de postes de iluminação dotados de inteligência capaz de fazê-los economizar energia e do uso de sistemas de monitoramento em tempo real de dados sobre fatores como trânsito e poluição. Cidades inteligentes também podem ampliar a transparência e a participação popular, a partir de mecanismos de consulta pública, de políticas de dados abertos, assim como gestores podem adotar sistemas inteligentes para potencializar a eficiência da administração pública (LISDORF, 2020).

---

[6] "A smart city uses digital technology to connect, protect, and enhance the lives of citizens. IoT sensors, video cameras, social media, and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions.". Tradução livre.

Desse modo, David Eckhoff e Isabel Wagner (2018) sumarizam as áreas que podem ser abordadas pelas cidades inteligentes em: mobilidade, sustentabilidade, economia, utilidades, serviços públicos, saúde, construção civil, governança e cidadania. Argumenta-se que as definições de cidade inteligente trazidas pelo setor privado costumam focar no ideal de cidade digital, dando protagonismo à aplicação da tecnologia (MOURA; DE ABREU E SILVA, 2019). As definições apresentadas pelas empresas são importantes para conhecermos as tecnologias aplicadas concretamente nas cidades, mas não são úteis para uma reflexão crítica sobre o modelo de cidade inteligente que queremos adotar enquanto sociedade.

As conceituações comumente trazidas pelo setor público não são muito diferentes em conteúdo, elencando aplicações possíveis da tecnologia no tecido urbano, mas costumam ser mais centradas nos interesses do cidadão, mencionando as realidades locais e as necessidades dos habitantes. É o caso da Carta Brasileira para Cidades Inteligentes (CBCI), elaborada com a intenção de definir uma estratégia nacional para a construção de cidades inteligentes, partindo do pressuposto de que a definição do termo é essencial. Buscando servir de insumo para gestores públicos, setor privado, legisladores e profissionais técnicos, a CBCI define cidades inteligentes como:

> (...) 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 e, em sentido amplo, do direito à cidade.

Já o Parlamento Europeu, em seu relatório sobre as cidades inteligentes da Europa, define a *smart city* como a cidade que busca abordar problemas a partir de soluções baseadas nas TIC e a partir de parcerias envolvendo diversos atores em

escala municipal. Os componentes utilizados nas cidades inteligentes incluem os recursos tecnológicos, materiais, financeiros, organizacionais e técnicos que devem ser pensados em três verticais: tecnologia, pessoas e instituições (EUROPEAN PARLIAMENT, 2014). Porém, segundo o documento, as definições podem focar no componente tecnológico ou em um contexto mais amplo de promoção da qualidade de vida ou o combate a defeitos urbanos.

Diante dessa amplitude, Kitchin (2015) define que existem três visões sobre cidade inteligente: a primeira, focada no papel da tecnologia e na incorporação de dispositivos à arquitetura, com o objetivo de extrair conhecimento sobre a cidade. Uma segunda linha foca na política pública urbana e na promoção de melhorias na infraestrutura, sustentabilidade, transporte, entre outros. Já a terceira vertente é centrada no cidadão, servindo de contrapeso aos interesses públicos e privados e defendendo bandeiras de justiça social. Essas três maneiras de pensar a cidade inteligente não são ontologicamente positivas ou negativas. É natural que elas existam e, quando combinadas, a tendência é que o resultado seja mais eficiente e inclusivo. Com foco nessa cooperação, o autor lista as promessas e os perigos trazidos pelas cidades inteligentes (ver Tabela 1).

Promessas	**Perigos**
Economia inteligente que fomenta empreendedorismo, inovação, produtividade e competitividade	Adoção de um discurso universalista que despolitiza e descontextualiza a vida urbana, priorizando soluções que podem ser desconectadas da história, cultura e política locais
Governo inteligente capaz de tomar decisões informadas, oferecer melhores serviços, sendo mais transparente, participativo e dotado de *accountability*	Utilização de discurso que considera dados, algoritmos e tecnologia como puramente técnicos e não ideológicos ou enviesados
Mobilidade inteligente, a partir da criação de sistemas eficientes, interoperáveis e multimodais de transporte público	Inversão do fluxo de solução de problemas (solucionismo), oferecendo soluções prontas que supostamente se aplicam em qualquer lugar de forma lógica e racional
Sustentabilidade inteligente, ao promover a economia de recursos e energia renovável	Esvaziamento da relevância do poder público, que pode tornar-se um consumidor de soluções privadas pré-prontas
Habitações inteligentes capazes de potencializar a qualidade de vida, a segurança e reduzir o risco de acidentes domésticos	Utilização de soluções tecnológicas mal desenvolvidas ou vulneráveis, representando risco de *bugs* ou de invasões por *hackers* que podem ter efeitos graves no mundo físico
População inteligente dotada de mais informação, potencializando a criatividade, inclusão, empoderamento e participação	Promoção de consequências negativas da economia movida a dados, como a vigilância, a erosão da privacidade, o perfilamento da população, entre outros

Tabela 1: Promessas e perigos das cidades inteligentes. Fonte: KITCHIN, 2015.

Neste trabalho, objetivamos mapear as principais formas de tratamento de dados dos cidadãos urbanos para entender como as informações sobre o ser humano se expõem nessa nova forma de convivência movida a dados pessoais. Em vez de discutirmos a ontologia da cidade inteligente, faz-se necessária uma definição funcional, que entende qual é o "DNA" tecnológico das cidades inteligentes, para então propormos alternativas técnicas e jurídicas para a mitigação do dano aos direitos dos cidadãos.

O ponto de vista adotado é oferecido pela especialista em governança digital Lilian Edwards (2016), que argumenta que as cidades inteligentes combinam as três tecnologias que mais ameaçam a privacidade no presente, quais sejam, a internet das coisas (IoT), o *big data* e a computação em nuvem. As *smart cities,* sem exceção, dependem da interação entre objetos dotados de conectividade, que passam a ser "inteligentes" (IoT). Toda essa informação gera um volume expressivo de dados de natureza variada, que são analisados de forma precisa e veloz (*big data*)*,* demandando uma sofisticada estrutura de armazenamento e processamento (computação em nuvem).

Edwards (2016) argumenta que essas tecnologias representam desafios para os quais ainda temos poucas soluções regulatórias, como o tratamento de dados sem consentimento no ambiente urbano, a falta de transparência sobre a finalidade e tempo de armazenamento de informações em *big data* e a dificuldade de garantir a segurança da informação em dispositivos de IoT. Tais funcionalidades serão estudadas com maior profundidade nos próximos capítulos, mas podem ser resumidos da seguinte forma:

- **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. Ainda, a competição entre cidades por recursos fomenta uma postura mais agressiva de adoção de mecanismos inteligentes, dificultando a discussão sobre os impactos sobre a privacidade (EDWARDS, 2016).

Tais fatores respondem à pergunta sobre qual é a relevância de discutir as cidades inteligentes. Em vez de uma simples discussão isolada sobre o uso de IoT, *big data* e computação em nuvem, as cidades inteligentes representam uma síntese inédita do uso de uma variedade de tecnologias que representam um relevante mercado global e possuem impacto direto sobre a vida das pessoas no presente. Logo, no próximo capítulo, será abordada especificamente a questão dos impactos à proteção de dados pessoais nas cidades inteligentes.

3. Proteção de dados nas cidades inteligentes

Direitos são construídos de acordo com a linguagem e os valores da época de sua fundação, sendo necessária a adaptação de seu conteúdo à medida que o tempo passa. Esta adaptação não ocorre somente em razão de mudanças culturais que refletem na alteração da lei, já que a evolução da tecnologia também interfere nos limites do direito, exigindo novos mecanismos para a regulação dos efeitos trazidos por essas descobertas. No que concerne à privacidade e proteção de dados, podemos dizer que estes dois fatores influenciaram o seu conteúdo. Aquilo que entendemos como "vida privada" e as ferramentas capazes de influir nos limites dessa privacidade sofreram mudanças, que causam uma dificuldade de delimitação sobre o que deve ser entendido como direito à privacidade.

Neste capítulo, abordaremos a evolução do conceito para contextualizar de que maneira podemos entendê-lo nas cidades contemporâneas. Em seguida, serão analisadas as dificuldades trazidas pela cidade interconectada no respeito à garantia da proteção de dados e aos riscos de cibersegurança que cada vez mais se manifestam na malha urbana. Por fim, analisaremos a experiência nacional a partir da LGPD e da Carta Brasileira de Cidades Inteligentes.

3.1. O direito à privacidade em espaços públicos

Alan Westin (2018) traça a genealogia do direito à privacidade, delimitando que o conceito, comum na retórica jurídica contemporânea, não é uma construção espontânea ou natural da convivência humana. Ao contrário, a gênese de um direito à não intromissão pode ser facilmente demarcada no tempo, tendo sua origem na segunda metade do século XIX, período de ampla juridificação de fenômenos sociais (DONEDA, 2019).

Westin (2018) expõe, por exemplo, que tribos de origem samoana não possuem um conceito de privacidade semelhante ao contemporâneo: as casas não tem paredes internas, os familiares dormem no mesmo cômodo e eventos da vida "natural", como a morte, a evacuação e o sexo podem ocorrer na presença de terceiros. O mesmo pôde ser analisado em uma variedade de sociedades pré-capitalistas, evidenciando que a elaboração de um aparato jurídico determinado a

proteger a vida privada é recente, visto que tal valor não goza de prioridade em diversas formas de sociedade.

Sem necessidade de tanto distanciamento geográfico do mundo ocidental, na Europa pré-industrial o conceito de privacidade era muito mais restrito. Nas vilas e cidades do feudalismo, a vida de uma família era um livro aberto para as demais famílias da região (FINCH; TENE, 2016). Sennet (2021) expõe, por exemplo, que, na Paris medieval, não existia qualquer estranhamento na comunicação espontânea entre estranhos e que as ruas eram marcadas por símbolos que demarcavam características privadas da vida de um indivíduo (por exemplo, as vestes eram utilizadas para marcar profissões tradicionais).

É somente com o desenvolvimento do capitalismo industrial, inspirado no individualismo liberal, que surge uma demanda por proteção da esfera íntima, com fundamento nos direitos da personalidade e no direito à propriedade, com ligação a proteção dos conceitos de "corpo" e "domicílio" (MULHOLLAND, 2019). Neste momento, a evolução tecnológica trouxe fatores que passaram a ameaçar a intimidade valorizada pelo ideário burguês do mundo industrializado, pois inovações como a fotografia instantânea e o jornalismo de massas fizeram proliferar as intromissões na vida privada das pessoas (DONEDA, 2021).

Diante da multiplicação de casos envolvendo tais controvérsias, os juristas estadunidenses Warren e Brandeis (1890) publicaram o artigo intitulado "*The Right to Privacy",* buscando dar robustez ao conceito. O artigo tornou-se um marco, inaugurando o chamado *right to be left alone*, ou seja, o direito de ser deixado só, sem que seja perturbada sua tranquilidade e intimidade. Sua argumentação se pauta na falta de rigor dos tribunais da época, que julgavam casos sobre colunas sociais e *paparazzi* que agrediam a intimidade de pessoas célebres. Porém, a primeira concepção de privacidade, ainda que inaugure a discussão jurídica, é limitada às demandas de uma burguesia privilegiada capaz de exigi-la, em contraste aos operários das grandes cidades, vivendo em moradias coletivas e superlotadas, sem qualquer privacidade (DONEDA, 2019).

Este conceito "negativo", ou seja, que busca garantir a intimidade de uma pessoa ou domicílio contra uma invasão alheia, se soma a outro fator decorrente da rápida urbanização do século XIX. Nas novas cidades, torna-se impossível distinguir um sujeito dentro da multidão urbana e as ruas passam a oferecer uma dimensão de anonimidade que antes era impossível. Sennet (2021) explica que a

necessidade de distinção social é trocada pelo mar de estranhos vestidos de preto, os quais não se conhecem e não interagem.

A moda passa a ser o uso de peças costuradas em série, potencializando a sensação de que a multidão é uma só, dificultando a identificação de um indivíduo específico. As cores que marcavam as ruas no Antigo Regime são trocadas pelo preto, criando a imagem de uma massa uniforme nas calçadas. A cidade se torna, então, um local de liberdade, uma possibilidade de fuga da vida provinciana marcada pelos laços sociais, econômicos e familiares. Essa sensação de '*nós'* faz com que o indivíduo anônimo espere que não seja identificado ou responsabilizado, permitindo que as pessoas se fechem sobre si mesmas, revelando pouco sobre sua intimidade (SENNET, 2021).

Ou seja, ainda que o *right to be left alone* não pudesse ser reclamado em espaços públicos, onde a expectativa de privacidade era quase nula, o que se verificava de forma prática era completamente distinto. Enquanto as comunidades rurais circulavam informação de forma horizontal através das trocas cotidianas, a vida nas sociedades urbanas passa a permitir uma proteção dos cidadãos contra as sanções sociais impostas pela comunidade (FINCH; TENE, 2016).

Com o tempo, o direito de ser deixado só se torna insuficiente diante das inovações tecnológicas e alterações na dinâmica social. A privacidade, que era entendida através do "*zero relation*", buscando garantir a ausência total da interferência de terceiros na vida privada, não oferecia uma defesa suficientemente forte contra a intromissão do Estado, agora dotado de formas de processamento de dados mais potentes. Nos anos 1960, com o surgimento da computação, a privacidade vira, também, uma questão de relevância existencial e coletiva. À privacidade "negativa" e individualista, soma-se uma dimensão positiva e socialmente relevante, ao mesmo tempo sendo oponível ao Estado e conectada com o exercício da autonomia pessoal (DONEDA, 2019).

Esta nova visão se baseia no conceito de "autodeterminação informativa", cunhado pelo Tribunal Constitucional Alemão em 1983, em caso envolvendo o processamento de informações pelo Estado. Ingo Sarlet (2021) explica que o caso caracteriza a privacidade como uma garantia da liberdade frente à repressão estatal, ao mesmo tempo que insere uma dimensão existencial ao debate, conectando a autodeterminação informativa a um direito que o cidadão possui de controlar a utilização de dados que dizem respeito a sua personalidade.

Especialista na discussão sobre direito e tecnologia, Stefano Rodotà (2007) considera que a dimensão negativa da privacidade não perdeu relevância, mas que, a ela, somou-se um direito que o indivíduo possui para atuar positivamente no controle do processamento de seus dados pessoais. Esta nova dimensão, que se adiciona à defesa da intimidade e sigilo, é chamada de proteção de dados pessoais, conectando-se às novas condições de circulação e controle da informação na nova realidade econômica dos anos 2000 (SARLET, 2021).

A doutrina de Rodotà é essencial no presente, quando presenciamos a constituição da economia movida a dados e baseada na extração e processamento da maior quantidade possível de dados pessoais. A forma como se trata dados, no presente, vai muito além do individual, sendo questão coletiva de relevância política e econômica. O surgimento da *internet*, nos anos 1990, teve influência direta na edição de normas ligadas à visão de que o aumento do fluxo de dados entre entes públicos e privados demandava uma nova regulação da privacidade. É o caso da edição da Diretiva 95/46/CE pelo Parlamento Europeu no ano de 1995[7], que veio a influenciar a criação do Regulamento Geral de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados, representantes europeia e brasileira de normas que buscam regular o tratamento de dados de uma forma completa.

Logo, ao falarmos de cidades, um conceito de privacidade individualista é insuficiente. Uma *smart city* é permeada por uma infinidade de sensores, controlados pelos setores público e privado, capazes de capturar e enviar informações sobre o ambiente e as pessoas que ali transitam. Por mais que o habitante urbano, em público, também goze da proteção da sua intimidade, trata-se de um fenômeno coletivo, que pretende influenciar a cidade como um todo para promover melhorias na qualidade de vida. Neste cenário, falar em *direito de ser deixado só* não basta, sendo essencial que os cidadãos sejam protegidos por legislações capazes de garantir direitos aos cidadãos de forma proativa.

> No contexto das cidades inteligentes, é importante salientar que a dimensão coletiva da proteção de dados se torna particularmente relevante. A estratificação de pessoas em grupos usando técnicas automatizadas para criação de perfis com o objetivo de prever o comportamento destes grupos pode escapar da perspectiva

[7] "Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados". Disponível em: https://eur-lex.europa.eu/legal content/PT/TXT/?uri=celex%3A31995L0046. Acesso em 19 de fevereiro de 2022.

> tradicionalmente individual de proteção de privacidade e do conceito de dados pessoais definidos pelo artigo 5º, I da nova Lei Geral de Proteção de Dados. (LGPD) (DONEDA; BELLI, 2021, p. 68).

Entretanto, ainda que possamos falar de proteção de dados nas cidades inteligentes, existem diversos desafios. Conforme exposto, 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 em meio à 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 dispositivos dotados de IoT e de assistentes domésticos conectados) e permitem localização e identificação de um indivíduo em meio à multidão (a partir de circuitos fechados de 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 para bases de dados privadas ou operadas em parceria com o setor privado, como os centros de controle espalhados em projetos de cidade inteligente (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 carregamos conosco de forma constante, 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 incrível precisão (SETO, 2015).

Casos como esse demonstram que nosso vocabulário jurídico ainda é limitado ao lidar com os desafios relacionados ao âmbito de incidência da privacidade. Segundo Koops (2014), o conceito de privacidade encontra-se em um dilema, já que seus limites foram profundamente alterados pelas novas tecnologias.

O autor argumenta que todo conceito jurídico tem fronteiras que marcam a sua incidência, podendo estas serem mais concretas ou abstratas. Estes marcadores podem perder a utilidade com o tempo, caso sejam baseados em conceitos defasados dos usos cotidianos.

A privacidade ainda se liga a dois conceitos cujas fronteiras mudaram drasticamente, quais sejam, "corpo" e "espaço privado". Para Koops (2014), a privacidade é o processo de tornar-se mais ou menos acessível para terceiros, sendo o espaço individual (com o corpo ao centro) e o território (com o lar ao centro) as fronteiras para sua delimitação. Enquanto o corpo está cada vez mais conectado à tecnologia, os limites territoriais entre o que é público ou privado se tornam nebulosos. Logo, a definição de vida privada com base no conceito de local não mais se sustenta, sendo impreciso afirmar que um indivíduo está mais ou menos exposto com base em sua localidade, o que se dá em razão de dois fenômenos que se verificam nas *smart cities*.

Em primeiro, o lar não é mais um ambiente onde somente a vida privada ocorre, já que a vida que se constitui dentro do lar flui para fora através dos diversos dispositivos que contém dados pessoais. Em segundo, a vida privada se encontra cada vez mais exposta no espaço público. Mesmo que a privacidade na cidade seja reduzida, indivíduos gozam de proteção legal da sua intimidade e esta proteção exigia menor esforço em razão da anonimidade proporcionada pela coletividade. Antes, podíamos esperar ser somente mais um rosto na multidão, mas hoje somos detectáveis através de uma variedade de recursos.

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.

Evans (2018) pondera que somente poderemos entender como abordar a questão da privacidade em *smart cities* ao entender que o conceito foi "desespacializado", ou seja, desvinculado de um caráter necessariamente espacial. Isto pois o fenômeno do *big data* e da economia baseada em dados depende da

transformação de objetos e pessoas em receptores e emissores constantes de informação, sem depender do local em que se encontram.

Por mais que a conceituação sobre o que é espaço público ou privado tenha variado, estes domínios historicamente são entendidos como separados. A privacidade foi construída com base na separação entre esfera pública e privada, o que se intensificou após o Iluminismo e a demanda pela proteção da propriedade e do lar (EVANS, 2018). Já no presente, o espaço privado é, também, um produtor de dados que serão analisados por terceiros, embaralhando o que é ou não íntimo. Evans argumenta que, como a estrutura econômica contemporânea depende do posicionamento do indivíduo como produtor de dados, a inserção deste indivíduo no espaço promove uma alteração da sua esfera privada. Isto pois as TIC já não operam em uma lógica interessada – ou até capaz - de diferenciar o espaço público do privado. Leia-se:

> A tecnologia digital, ao mesmo tempo, coexiste com o usuário em espaços privados, mas também é responsável pela transformação das atividades das pessoas nos espaços privados, tornando público o que é privado e apagando os parênteses do privado, em uma redução de todas as esferas da atividade humana à produção de dados. (EVANS, 2018, p. 6).[8]

Sendo assim, é necessário termos cuidado ao falar de "privacidade e proteção de dados nas cidades inteligentes", sob risco de estarmos abordando um fenômeno recente com lentes do passado. Não se nega a relevância das dimensões corporais ou espaciais da privacidade, visto que estas guardam importância e seguimos não desejando intromissões indesejadas em nosso espaço privado. Contudo, é necessário entender que o rápido avanço da tecnologia põe em risco a utilidade dos conceitos empregados, a não ser que tragamos maior rigor ao seu uso. Assim, com conhecimento dos sistemas utilizados com maior frequência nos projetos de *smart cities*, é possível entender o que significa a privacidade nas cidades e pensar a melhor forma de proteger os dados dos cidadãos.

[8] "Digital technology is both co-existing with the user in private spaces but also responsible for a transformation of the activities of people in private spaces that renders the private public, and erases the parenthesis of the private in a genereal flattening of all spheres of human activity as data-producing". Tradução livre.

Neste sentido, Martinez-Ballesté et al. (2013) buscaram elaborar uma definição de privacidade compatível com as cidades inteligentes[9], dividindo-a em dimensões de modo a entendê-la de forma coerente com o problema concreto abordado. Os autores negam que cidades inteligentes são uma ameaça intrínseca à privacidade, trazendo formas de efetivar tanto sua construção quanto a proteção de dados. Para isso, combinam modelos desenhados para bases de dados e para serviços baseados em localização (LBS)[10], tecnologias comuns às cidades inteligentes, gerando um terceiro modelo que busca dimensionar e abordar a privacidade na cidade inteligente como um todo.

Ao tratar de bases de dados, Martinez-Ballesté et al (2013) trazem a moldura 3D, com a privacidade representada em três dimensões complementares: a privacidade dos titulares cujos dados estão armazenados na base de dados (*respondent privacy*), a privacidade das consultas (*queries*) realizadas por quem acessa a base (*user privacy*) e a privacidade do proprietário dessas bases, que pode delimitar o nível de acesso que cada usuário terá aos dados nela armazenados (*owner privacy*).

Para os LBS, utiliza-se o modelo W3 *(where, what who*), baseado premissa de que, no uso destes sistemas, "alguém está pedindo por alguma coisa em algum lugar"[11], demandando a proteção de três dimensões: o "onde" (privacidade de localização), o 'que*'* (o que este usuário está consultando, ou privacidade de consultas) e o 'quem' (privacidade de identidade). Combinando os modelos, surgem 5 dimensões (5D), incluindo a privacidade de: identidade, consulta, localização, pegadas digitais e do proprietário. Segundo os autores, isto permite que a cidade inteligente seja abordada a partir de uma moldura que entende as diferentes formas de privacidade envolvidas, permitindo que se elaborem soluções destinadas a cada uma delas.

---

[9] A definição trazida por Ballesté é a mais utilizada pela literatura que busca estudar formas de mitigar os danos à privacidade nas cidades inteligentes. Contudo, outros autores já propuseram formas distintas de decomposição da privacidade. David Eckhoff e Isabel Wagner (2018), por exemplo, separam a privacidade em: privacidade de localização, privacidade de corpo e mente, privacidade da vida social, privacidade de comportamento e privacidade de meios digitais.

[10] São serviços que dependem da comunicação de um usuário localizado em um lugar identificado pelo seu dispositivo, que se conecta a um provedor de serviços em tempo real através de uma rede móvel (QU et al., 2018). Estes dados gerados, que combinam a identidade, a localização, o momento e o teor das consultas dos usuários, são armazenados em bases de dados variadas. São exemplos de LBS: sistemas de mapas, navegação, geolocalização e rastreamento, os aplicativos de previsão do tempo e as redes sociais.

[11] "Someone is asking for something somewhere" (BALLESTÉ et al., 2013). Tradução livre.

Dimensão de privacidade	Exemplo em *smart cities*
Identidade (diz respeito à revelação ou não da identidade do usuário quando este utiliza um serviço de cidade inteligente. Diz respeito a "quem" é o usuário. A especificação ou não da identidade permite determinar se este dado, ao ser correlacionado, poderá ser usado para mapear o titular)	Usuário informa a sua identidade ao acessar um estacionamento inteligente. Posteriormente, este dado é vazado e reutilizado para extrair informações sobre o titular. A maioria dos serviços utilizados em cidades inteligentes trazem preocupações relacionadas à identidade dos titulares.
Consulta (diz respeito à preservação da privacidade das consultas realizadas pelo titular a um serviço de cidade inteligente. Diz respeito ao "que" esse usuário busca. Ao coletar os pedidos realizados por um usuário, fornecedores de serviços podem perfilar titulares e colher informações sobre seus hábitos)	Cidadão interage com serviço municipal de informações, localizado em um poste inteligente, realizando consultas. Caso essas consultas sejam expostas, é possível reutilizar tais dados para análise de hábitos e perfil de um indivíduo.
Localização (é a preservação da privacidade da localização física do usuário. Diz respeito a "onde" o usuário se encontra. Estes dados podem ser usados para mapeamento de deslocamentos em tempo real ou para análise de padrões de deslocamento frequentes)	Um prédio inteligente, dotado de sistema de reconhecimento facial e registro automático de visitantes, é capaz de identificar a presença de um indivíduo em um momento específico ou de registrar que o mesmo indivíduo frequenta o edifício três vezes por semana. Estes dados podem revelar um padrão de deslocamento ou algum hábito específico.
Pegadas digitais (são as informações que podem ser obtidas ou inferidas a partir de conjuntos de metadados gerados a partir da atividade de um usuário. As atividades de cidades inteligentes dependem da extração, armazenamento e análise de quantidades massivas desses dados (*big data*). Os serviços de *smart cities* coletam informações geradas através do seu uso, que geram novas informações a partir da análise)	Um serviço de agendamento de consultas médicas na rede pública de saúde pode deixar traços capazes de conectar um cidadão a uma condição específica de saúde, violando a sua intimidade.
Propriedade de base de dados (Essa dimensão diz respeito ao proprietário da base de dados que é consultada por usuários ou entidades, podendo o controlador optar por compartilhar ou não as informações a depender do consultante. Esta dimensão é relevante para a interação entre serviços distintos em uma cidade inteligente, já que estes dependem da correlação de diversas bases de dados)	Uma companhia de eletricidade busca correlacionar o uso de energia com o uso de outros serviços, como gás e água. Essa interação envolve a conexão entre bases de dados controladas por atores distintos, que podem ou não optar por compartilhar suas informações ou delimitar o nível de acesso que será dado a outra parte.

Tabela 2 – Abordagem 5D para privacidade em smart cities. Fonte: MARTÍNEZ-BALLESTÈ et al., 2013.

A decomposição da privacidade em dimensões, no contexto de cidades inteligentes, é uma medida importante para não cairmos no lugar comum da "extinção da privacidade", que favorece a paralisação e a não abordagem dos riscos cotidianos da aplicação das TICs no tecido urbano. Um posicionamento reativo e generalizador acaba por ter a proibição das cidades inteligentes como única

alternativa, impedindo que o seu lado positivo, a promoção da qualidade de vida, seja efetivado. Ao compreender as dimensões que são impactadas, é possível pensarmos em soluções construtivas que busquem mitigar os riscos e potencializar os benefícios de cada estratégia. A seguir, iremos abordar quais são estes riscos postos pelas *smart cities*, em especial no que diz respeito à proteção de dados e à segurança das informações.

3.2. Desafios trazidos pelas *smart cities*

Como vimos, as *smart cities* mobilizam a retórica da utopia. A reação a tal retórica, questionando as aplicações concretas dessa utopia, é necessária para que se mitiguem as consequências negativas desse progresso. Por outro lado, é preciso cuidado para que a crítica não se faça distopia, simplificando fenômenos complexos como puramente negativos. Entretanto, conforme será exposto, o modelo hegemônico de *smart city* ainda possui deficiências de privacidade e segurança, o que pode trazer consequências adversas e dificultar a criação de uma relação de confiança com os cidadãos.

Por isso, estamos diante de um desafio bidimensional, que é tanto tecnológico quanto regulatório. A seguir, serão abordados os principais desafios trazidos pela aplicação da tecnologia nas cidades, sob a ótica da proteção de dados pessoais e da segurança das informações. Tais críticas serão realizadas como forma de diagnóstico dos riscos que a adoção acrítica das utopias pode trazer, evitando a assunção precipitada de que as cidades inteligentes significam, obrigatoriamente, um projeto de exacerbada vigilância.

3.2.1. Privacidade e proteção de dados

Para Hiller e Blanke (2017), o modelo dominante para as cidades inteligentes pode ser visto como um projeto de vigilância que desafia os limites da privacidade individual ao agregar e combinar dados para influenciar comportamentos. Por outro lado, os autores reconhecem que a *smart city* é um caminho não só inevitável como necessário[12], pois a experiência demonstra que

[12] Diante de cidades cada vez mais populosas e de iminentes desafios de ordem climática, argumenta-se que a cidade inteligente se faz necessária para enfrentamento mais qualificado e técnico destes problemas. Ou seja, apesar dos desafios na implementação da tecnologia ao tecido

tecnologias disruptivas não são ignoradas e tendem a ser utilizadas, especialmente diante de atrativos econômicos como os das cidades. Além disso, a tecnologia nos ajuda a enfrentar problemas urbanos contemporâneos, sendo nosso desafio cumprir suas promessas de forma responsável (KITCHIN, 2015).

As *smart cities* se alimentam de informação para influenciar e redirecionar a cidade rumo à eficiência e ao aumento de qualidade de vida. Apesar de certas aplicações terem sucesso com o uso de informação anonimizada, é fato que parte de sua estrutura dependerá de dados de indivíduos identificados ou identificáveis. Tal tratamento massivo de dados pessoais é fruto de uma rápida evolução tecnológica que limitou a capacidade de reagirmos de forma eficiente através da regulação (HILLER; BLANKE, 2017).

A principal preocupação da sociedade civil com a expansão do modelo de cidade interconectada é a possibilidade de expansão da vigilância, ou seja, do acesso facilitado a informações sobre deslocamentos, hábitos cotidianos e até informações sensíveis, como a participação em movimentos sociais e políticos ou detalhes sobre a vida íntima e a saúde (ANTONIALLI; KIRA, 2020). Ademais, estudiosos apontam a possibilidade de, além da descoberta de comportamentos, que a tecnologia seja usada para influenciar comportamentos através de direcionamento de informação e *nudges*[13] (HILLER; BLANKE, 2017).

A possibilidade de influenciar o comportamento dos cidadãos se alia a projetos de urbanismo de cariz paternalista, que se valem da dificuldade de separação entre o que é monitoramento e o que é manipulação de comportamentos (FINCH; TENE, 2016). Tal preocupação é ainda maior em países com históricos autoritários, já que a tecnologia invasiva é uma arma potente para a localização, identificação e eventual perseguição de adversários políticos. Ou seja, a

urbano, tal processo será inevitável para o enfrentamento dos principais desafios do futuro (abastecimento de água, poluição, superpopulação, desastres ambientais, entre outros). Nautiyal et al. (2018) argumentam que as necessidades futuras irão impelir as cidades para uma inevitável necessidade por inovação, o que impõe pensarmos, desde já, como lidar com as questões envolvendo a privacidade e segurança das informações.

[13] 'Nudge' é um termo que deriva da economia comportamental, indicando um processo que busque, muitas vezes de forma oculta, persuadir alguém a adotar um comportamento. É uma prática que depende da coleta de dados pessoais para o mapeamento dos hábitos das pessoas. Depois, esses hábitos mapeados são influenciados a partir de "empurrões", ou seja, nudges. As cidades inteligentes aumentam drasticamente a superfície em que cidadãos estão sujeitos a nudges, já que em qualquer lugar poderão enviar e receber estímulos através das tecnologias da informação e comunicação (KITCHIN, 2018).

materialização de uma *smart city* também traz desafios de ordem democrática[14], permitindo influenciar a opinião pública, detectar adversários ou monitorar a organização de movimentos sociais (MALLAN, 2015).

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 Bentham no século XVIII. Nele, um agente, posicionado ao centro, é capaz de observar todas as celas ao seu redor (BENTHAM, 1995). 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 (MALLAN, 2015). São evidentes as coincidências do panóptico com a cidade inteligente, em que cidadãos são facilmente identificáveis e localizáveis através de controles centralizados, além de seus comportamentos serem mensuráveis.

Atualmente, o planejamento de cidades inteligentes foca excessivamente nos usos dados à tecnologia, em detrimento de questões políticas envolvendo a coleta e uso de dados. A maioria dos *rankings* que medem a "inteligência" nas cidades não utiliza a privacidade como um indicador, o que se evidencia na ausência desse fator na maioria dos relatórios públicos sobre o fenômeno (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 pelos nossos dados.

Tal visão considera que toda informação é relevante para a cidade, devendo ser utilizada de forma igualmente incisiva. Contudo, as informações que fluem em uma *smart city* possuem diferenças no que diz respeito a titularidade, volume, finalidade, entre outras variáveis (VAN ZOONEN, 2016). Por exemplo: os dados coletados por um painel de energia solar disposto em uma praça são menos sensíveis do que aqueles extraídos de um *smartphone,* que podem expor detalhes da vida pessoal de seu usuário. Logo, não é porque temos facilidade em gerar dados que todos possuem o mesmo nível de risco.

[14] Por outro lado, não são poucas as oportunidades de potencialização da democracia por meio das tecnologias urbanas, que, imbuídas dos ideais da transparência, promoção do civismo e do livre fluxo da informação, podem ser utilizadas para reduzir a assimetria de poder entre o Estado e a sociedade e para facilitar a integração e organização da sociedade civil. Para maior aprofundamento no tema, sugerimos a leitura da obra "*The smart city in a digital world"* (MOSCO, 2019) e "*Smart cities as democratic ecologies*" (ARAYA, 2015).

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"[15] 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 vendidos – de forma legal ou ilegal – 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 (RENNÓ et al., 2016). Munidos desses dados, os agentes de tratamento conseguem traçar perfis, treinar algoritmos e interagir com os titulares de maneiras inéditas, principalmente através da publicidade comportamental (ANTONIALLI; KIRA, 2020).

Sabemos que a preocupação com a vigilância do Estado sobre o cidadão não é nova, apesar de ter sido potencializada com o surgimento das TICs, mas o fenômeno das *smart cities* traz um novo componente: a presença crescente do setor privado como figura capaz de observar, medir e influenciar os comportamentos dos cidadãos. Na internet, a prevalência do setor privado é evidente, mas, no mundo físico, seu apetite por dados pessoais já se manifesta.

Com a crescente presença do setor privado na prestação de serviços públicos e com a facilidade de disposição de sensores privados pela cidade, um número cada vez maior de bases de dados é operado pelo setor privado. A *smart city* permite ao setor privado tanto a atuação ao lado do Estado quanto facilita que atores privados, por si só, coletem dados através de câmeras e outros recursos instalados em suas

[15] 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).

propriedades (FIRMINO, 2018)[16]. Batty (2017) argumenta, inclusive, que o movimento das cidades inteligentes somente é possível diante da facilidade de disposição de tecnologia privada pela cidade, tornando nebulosa a fronteira entre o que é público ou privado no espaço urbano.

Os dados que são coletados a partir da interação do cidadão com a cidade inteligente são armazenados em um ambiente complexo, transitando entre o setor público e o privado sem que o usuário tenha clareza dos limites desse tratamento (FINCH; TENE, 2016). Essas formas privadas de coleta de dados trazem preocupações quanto à privatização de informações públicas, à falta de alternativa para os cidadãos e à falta de transparência do tratamento dos dados pessoais. Tendo em vista que a participação do cidadão nos processos de smart cities é condição necessária para uma relação de confiança, a descentralização da coleta de dados em silos privados torna mais difícil que o cidadão confie na cidade.

Van Zoonen (2016) alerta que a conexão cada vez mais próxima do setor privado com a operação de serviços públicos inteligentes gera o risco de que os objetivos do Estado passem a ser guiados pelos imperativos do mercado. Isto, segundo Edwards (2016), gera dúvidas sobre quem de fato é proprietário das bases de dados vinculadas às funções públicas. Essa falta de transparência é ainda mais grave diante de parcerias realizadas para fins de policiamento[17], vigilância ou

[16] A presença cada vez maior de câmeras privadas dotadas de reconhecimento facial apontadas para espaços públicos permite, por exemplo, que empresas possuam gigantescas bases de dados sensíveis coletados sem a anuência dos pedestres. Tal tipo de coleta de dados se soma àquela que ocorre quando uma empresa de tecnologia do setor privado passa a prestar um serviço público através de uma concessão. A Autoridade de Proteção de Dados da Noruega, por sua vez, já multou uma empresa em 15 mil euros pela transmissão contínua de uma de suas câmeras na internet, já que esta capturava imagens em 360 graus e registrava atividades em espaços públicos (Datatilsynet – caso 20/01627). Da mesma forma, a Autoridade de Proteção de Dados da Irlanda emitiu uma multa de 110 mil euros contra o município de Limerick, pelo uso indiscriminado de câmeras, *softwares* de reconhecimento de placas de carro e drones (DPC – caso 03/SIU/2018).

[17] Kitchin, Cardullo e Di Feliciantonio (2018) ressaltam que diversas forças policiais locais, nos EUA, estão utilizando análise preditiva para tentar antecipar a localização de crimes futuros e direcionar policiais para essas áreas. A cidade de Chicago, por exemplo, utiliza estatísticas de aprisionamento, registros telefônicos e dados de redes sociais para realizar perfilhamento tanto em escala macro (perfil de uma área) quanto de forma individualizada. Esses dados retroalimentam a lógica da violência urbana, direcionando a repressão para áreas excluídas e tornando mais difícil a ressocialização de pessoas com registros de antecedentes. Os autores ressaltam, também, que existe pouca clareza sobre como esses dados são utilizados nas cidades, afirmando que forças policiais monitoram comunicações entre ativistas e tentam controlar movimentos sociais. Ainda, Halegoua (2020) traz o exemplo da tecnologia *ShotSpotter* ("localizador de disparos") já aplicada em cidades pelos EUA. A instalação de um sensor de disparos foi criticada pelos habitantes de San Diego, que consideraram que o sistema foi instalado sem consulta popular e prejudica a relação de confiança entre os habitantes e a cidade. A iniciativa foi criticada por fazer com que o policiamento se torne excessivamente dependente de tecnologias, suplantando o policiamento comunitário e encorajando a atuação distanciada pelos agentes. O uso da aplicação foi criticado até por agentes de segurança,

serviços de emergência, que dependem de dados politicamente sensíveis, como registros de reuniões públicas ou registros criminais.

Ainda, os serviços urbanos não são pensados de forma que priorize a proteção dos dados armazenados, não havendo, na maioria dos casos, protocolos de interoperabilidade[18] entre as bases de dados de uma cidade, favorecendo a obscuridade e a concentração da informação (EDWARDS, 2016).

Em razão dessa opacidade, algumas empresas buscam utilizar a garantia da privacidade como diferencial competitivo, oferecendo opções de produtos que supostamente dão maior valor à privacidade do usuário. Finch e Tene (2016) alertam que mesmo essa pequena fatia de mercado dedicada ao respeito da privacidade dificilmente irá penetrar na estrutura das *smart cities*, já que o fornecimento de serviços urbanos é um setor monopolista por excelência. O setor privado de tecnologia também é concentrado em pequenos grupos como as Big Five (Amazon, Google, Microsoft, Facebook e Apple), assim como o setor de IoT é concentrado em poucas empresas, como Cisco e IBM[19]. Ou seja, as cidades não possuirão, por exemplo, mais de um serviço inteligente de transporte público, não havendo como o cidadão optar por aquele que considera mais segura.

Além de não possuir opções de mercado, mesmo que o cidadão opte por configurações pessoais que priorizem a proteção de dados, é improvável que este consiga se evadir da infraestrutura entrelaçada de sensores. Se não inserirmos a defesa da privacidade no debate sobre as *smart cities*, é razoável esperar que haverá uma substituição da lógica *privacy by default* pelo *tracked by default* (FINCH; TENE, 2016). Ou seja, a arquitetura da cidade será desenhada seguindo a lógica da economia movida a dados, na qual os hábitos consumidores são constantemente analisados, pondo em risco o seu poder de decidir como serão tratados os seus dados (ECKHOFF; WAGNER, 2018).

---

pois vai contra o ideal de policiamento preventivo, cuja forma de ação deve buscar prevenir os disparos em vez de agir após a sua localização.

[18] A Comissão Europeia (EUROPEAN COMMISSION, 2021) entende que a interoperabilidade entre serviços de cidades inteligentes é um dos principais desafios para a garantia de sucesso desses projetos, sendo passo essencial para que os serviços de *smart city* sejam prestados de forma transparente, eficiente e sustentável. Por este motivo, o órgão produziu, no ano de 2021, uma proposta de arquitetura de interoperabilidade para cidades inteligentes europeias, colacionando uma extensa lista de propostas para tal fim.

[19] Segundo o portal IT Chronicles (2021), as 5 principais empresas de smart cities são, além da Cisco e IBM, a Siemens, Huawei e Microsoft.

A ausência de concorrência faz com que os cidadãos tenham pouca clareza sobre o destino dos seus dados, bem como sobre os usos e reutilizações destes. Além do dano aos direitos dos titulares, isto representa um ônus democrático no que diz respeito ao acesso do cidadão à informação mantida pelo Estado (FINCH; TENE, 2016). A pesquisa sobre cidades inteligentes conclui que um dos principais desafios para a manutenção da sustentabilidade destas é a garantia da confiança do cidadão quanto às atividades de tratamento. Assim, Elvira Ismagilova et al. (2019) consideram que, sem o equilíbrio das iniciativas com a garantia de direitos, a cidade inteligente não contará com o apoio e a confiança da sociedade civil.

A erosão da confiança tende a aumentar caso o cidadão não tenha clareza sobre as tecnologias aplicadas nas cidades, especialmente em uma sociedade cada vez mais ciente dos vieses e deficiências reproduzidos em certos algoritmos. O uso da inteligência artificial adiciona outra camada à falta de transparência das cidades, pois, além de não saberem como dados são armazenados ou usados, os cidadãos também não conhecem o critério de tratamento dessas informações. Mulholland e Frajhof (2020) entendem que o avanço da inteligência artificial e aprendizado de máquina demandam uma resposta regulatória capaz de fornecer transparência ao uso dessas tecnologias. Assim, no contexto urbano, é razoável esperar que os cidadãos possam demandar explicação sobre como sua informação é tratada, indo em linha com o direito à revisão de decisões automatizadas, que será abordado com maior profundidade neste trabalho.

Além da dificuldade de entendimento com relação ao tratamento de dados, sabemos que o mal uso das novas tecnologias permite a potencialização de discriminações já existentes, bem como a criação de novos padrões discriminatórios que podem se esconder por detrás da ciência de dados. Apesar de serem tratados como frutos de uma ciência objetiva e imparcial, os códigos que estruturam os sistemas das cidades são criados por seres humanos, podendo reproduzir – intencionalmente ou não - preconceitos que o desenvolvedor carrega, criando algoritmos enviesados (BRAGA, 2020).

O treinamento de algoritmos com dados dos cidadãos deve ser feito com cautela, pois os dados gerados na *smart city* são de grande volume e heterogeneidade, sendo difíceis de interrelacionar e de gerar conclusões objetivas e confiáveis. Para Ismagilova et al. (2019), a baixa qualidade dos dados de cidades inteligentes pode prejudicar a eficiência e acurácia das análises realizadas. Quando

unimos dados de baixa qualidade com algoritmos obscuros, existe o risco real de que as cidades inteligentes venham a reproduzir preconceitos já introjetados na sociedade (RODRIGUEZ, 2019). Isto pode ser ainda mais grave em países marcados pelo racismo, pela desigualdade e pela violência urbana, nas quais os sistemas de *smart cities* podem reforçar a marginalização já existente (BRAGA, 2020).

Ainda sobre a discriminação, esta poderá se materializar em razão dos diferentes níveis de interação com a cidade. Pessoas de classes mais pobres, idosas ou portadoras de deficiência podem ter dificuldade de produzir dados e usar serviços digitais. Em Boston, por exemplo, verificou-se que o aplicativo *Street Bump,* usado para localizar buracos nas ruas, não direcionava reparos com a mesma frequência para bairros de população empobrecida ou idosa, já que estes não interagiam com a plataforma (FINCH; TENE, 2016). Logo, caso um cidadão não interaja com a cidade inteligente, é possível que a sua cidadania seja limitada (ISMAGILOVA et al., 2019), reforçando que a troca de dados por serviços mais eficientes não é verdadeira, não havendo troca livre, mas a imposição de condições para acessar serviços públicos.

A utilização de dados para o melhoramento da qualidade de vida urbana e para o aumento da eficiência do Estado não é um fenômeno recente. A diferença contemporânea está na escala, já que estes dados abrangem uma área muito maior e fluem de maneira muito mais rápida, permitindo a criação de bases de dados complexas e com um nível profundo de detalhes sobre a vida dos cidadãos. Tal evolução só é possível, conforme exposto, pela multiplicação de dispositivos conectados à internet, pela internet das coisas, pela análise de *big data* e pelo armazenamento em nuvem (ANTONIALLI; KIRA, 2019), tecnologias que trazem sérias dificuldades para a proteção de dados pessoais.

A internet das coisas (IoT) é certamente um dos principais fenômenos a possibilitar a existência de uma *smart city*, pois objetos cotidianos passam a serem capazes de receber e emitir informações em tempo real. Um relógio passa a ser capaz de medir dados vitais de um usuário ou rastrear o seu deslocamento, assim como uma rede inteligente de energia elétrica gera dados que permitem inferir os hábitos dos residentes de algum imóvel (RODRIGUEZ, 2019).

O principal problema dos dispositivos de IoT não é um defeito, mas sim uma característica de seu *design*. Estes objetos foram pensados para permitir a

interação espontânea com o usuário, o que os leva a serem discretos e de uso facilitado. Os dispositivos de *smart home*, por exemplo, funcionam de forma aparentemente inerte, registrando as preferências dos habitantes para personalizar o serviço. Finch e Tene (2016) argumentam que, em escala urbana, isto representa um risco de que a coleta de dados se integre à arquitetura da cidade sem que os cidadãos percebam. Essa discrição dificulta a criação de expectativa dos cidadãos quanto à coleta de dados e a maioria das interações dos humanos com a IoT será despida de avisos de privacidade, sendo difícil que o usuário entenda os limites do tratamento ou possa exercer seus direitos (EDWARDS, 2016).

Em seguida, o espalhamento de dispositivos de IoT permite a coleta, armazenamento, venda, manipulação e reutilização uma quantidade incrível de dados, criando o *big data* urbano que sustenta as cidades inteligentes (HILLER; BLANKE, 2017). Quanto ao termo, Batty (2015) argumenta que as definições de *big data* que se baseiam somente no volume de dados são falhas, porque tornam-se rapidamente defasadas. Na cidade inteligente do futuro, aquilo que hoje chamamos de *big data* será considerado *small data*.

Segundo Kitchin (2014), devemos entender *big data* como: gigante em volume, tratado em alta velocidade, de variedade diversa, de escopo exaustivo (ou seja, que busca coletar todos os dados possíveis sobre um fenômeno), de resolução precisa, facilmente relacionável e flexível. É esse tipo de dado que é utilizado, nas cidades, para analisar os fenômenos urbanos e os hábitos dos cidadãos, sendo compartilhado pelos setores privado e público com intenção de fornecer serviços à população (HILLER; BLANKE, 2017).

Para Michael Batty (2015), a característica distinta do *big data* é a possibilidade de coletar e transmitir estes dados em tempo real. Essa versatilidade permite às cidades inteligentes a criação de centros de análise de dados, com *dashboards* e medidores precisos, como no Centro de Operações do Rio de Janeiro. Não é difícil de entender por que construções como o COR-Rio remetem ao panóptico benthamiano, já que a partir de uma única sala é possível observar, em tempo real, uma quantidade amplíssima de pessoas e lugares.

Mas, para que não caiamos em lugares comuns, precisamos delimitar as preocupações com relação ao tratamento de *big data* nas cidades inteligentes. Segundo Lilian Edwards (2016), estas são: a possibilidade de reidentificação de dados anonimizados, a reutilização dos dados para finalidades distintas da coleta, a

falta de transparência, a coleta de dados excessivos e o uso de dados de baixa qualidade. São características que não respeitam princípios previstos pela LGPD, como a qualidade, necessidade, finalidade e transparência, que serão explorados a seguir (item 3.3).

Por fim, esses dados dependem da estrutura de computação em nuvem para serem acessados, compartilhados e armazenados. A nuvem, segundo a norma ISO/IEC 17.788:2014, é o sistema que permite o acesso a um grupo de recursos ajustáveis e elásticos, que podem ser físicos ou virtuais e podem ser compartilhados (RODRIGUEZ, 2019). Ou seja, são recursos de acesso amplo, separados em grupos, cujo acesso independe de um administrador centralizado. Os serviços de *cloud* se diferenciam por serem disponíveis em velocidade elevada e permitirem a "compra" de armazenamentos de grande escala (*software as a service*) por qualquer um que desejar (EDWARDS, 2016).

As nuvens trazem riscos à proteção de dados, pois a concentração de informações no mesmo repositório torna um eventual incidente muito mais grave, afetando um alto número de cidadãos. Além disso, a *cloud* não se limita ao armazenamento dos dados da cidade inteligente, mas fornece uma estrutura que permite o seu processamento de forma rápida, multiplicando tanto os benefícios quanto os riscos deste tratamento (RODRIGUEZ, 2019). Quanto à transparência, a *cloud* também traz desafios, já que os cidadãos não têm a capacidade de saber de que forma os seus dados serão armazenados, limitando a sua capacidade de exercer direitos. Isto é ainda mais grave quando levamos em conta que as nuvens utilizadas nem sempre estarão sediadas no mesmo país que o titular, trazendo dúvidas no que diz respeito à legislação aplicável (EDWARDS, 2016).

3.2.2. Segurança da informação

Durante a última década, a segurança das informações ganhou relevância, tornando-se um dos principais itens da agenda global de segurança. Casos como a manipulação das eleições americanas em 2016 e a denúncia de Edward Snowden sobre processos de espionagem levaram o tema às instâncias internacionais. Apesar da proximidade entre proteção de dados e segurança da informação, é equivocado entender que a garantia da primeira depende exclusivamente da segunda. Hoje, a discussão sobre proteção de dados superou a esfera técnica de garantia do sigilo e

prioriza a garantia dos direitos fundamentais do cidadão. Na consecução desse objetivo, a segurança da informação é uma obrigação acessória ou instrumental na garantia da proteção de dados (WIMMER, 2020).

A segurança da informação compõe o direito à proteção de dados, mas não trata das consequências planejadas de uma iniciativa, mas sim diz respeito à proteção da iniciativa contra ocorrências indesejadas pelo controlador e pelo titular. Assim, Miriam Wimmer (2020) explica que é possível que um mesmo banco de dados possua informação segura e dados desprotegidos, e vice-versa. Por exemplo: uma base de dados criptografada pode estar segura, mas o tratamento dos dados pode violar a LGPD. Ao inverso, um tratamento de dados pode ter objetivo lícito, enquanto o banco de dados se encontra vulnerável.

Quanto ao objeto de proteção, também há distinções:

> Em outra vertente, a segurança da informação preocupa-se com impactos econômicos, políticos e sociais decorrentes do acesso indevido a informações de natureza variada, incluindo dados pessoais e não pessoais; ao passo que as normas de proteção de dados pessoais voltam-se de maneira mais marcada para a proteção do indivíduo. (WIMMER, 2020, p. 135)

Para a homogeneização das abordagens ao tema, a Organização Internacional de Normalização (ISO) criou uma família de normas (ISO 27.000 e seguintes) para a definição dos conceitos e estabelecimento dos melhores padrões de segurança da informação, definindo segurança da informação como:

> Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006, p. 2).

Em geral, os três pilares da segurança da informação são a confidencialidade (informação não ser revelada a terceiros não autorizados), disponibilidade (informação estar acessível às pessoas autorizadas) e integridade (garantia da exatidão e completeza dos dados). Ainda, devemos entender os incidentes de segurança da informação como "*eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação*" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006, p. 2).

Hoje, o principal desafio para a garantia da segurança das informações é a descentralização dos atores. Uma abordagem que vise promover a segurança deve integrar governos nacionais, governos locais, empresas e a sociedade civil, sendo difícil atingir consensos sobre quais responsabilidades cabem a cada ator (HUREL, 2019). O problema é que, enquanto isso, a tecnologia avança e é implementada em velocidade impressionante, mesmo diante de riscos.

Nas cidades inteligentes, o risco é evidente, pois os incidentes não se restringem ao mundo digital, envolvendo sistemas ciber-físicos (*cyber-physical systems*). Estes são sistemas que integram sensores, computação e rede sobre objetos físicos e a infraestrutura, como os carros autônomos e as redes inteligentes de energia (*smart grid*) (NARAYANAN et al., 2019). Ataques a aplicações como essas possuem efeitos no mundo físico, podendo causar acidentes graves que afetam a integridade física das pessoas. A exposição de sistemas ciber-físicos permite, além da violação à privacidade e à integridade física, graves danos econômicos e reputacionais, podendo prejudicar a confiança dos cidadãos nas *smart cities* (NAUTIYAL; MALIK; AGARWAL, 2018).

Conectar a infraestrutura à internet significa que o acesso a esses sistemas pode ser feito de forma remota, permitindo acessos não autorizado a serviços essenciais. Nos últimos anos, alguns ataques chamaram atenção para a vulnerabilidade das cidades. Em 2015, por exemplo, a rede de energia elétrica da Ucrânia foi atacada por *hackers*, o que levou mais de 230 mil pessoas a ficarem sem acesso a eletricidade (CUI et al., 2018). No Irã, em 2012, um ciberataque foi direcionado às centrífugas nucleares do país, evidenciando a possibilidade de transformar a rede de serviços inteligentes em uma poderosa arma (HUREL, 2019). Em 2021, um grupo russo atacou o gasoduto Colonial Pipeline nos EUA, interrompendo os seus serviços por dias, causando crise de abastecimento. Também gera preocupação o setor da saúde (NAUTIYAL; MALIK; AGARWAL, 2018), pois incidentes interrompem a prestação de serviços essenciais, como no ataque à Fresenius, maior empresa privada de diálise da Europa (DIMOV, 2020).

Essas ocorrências demonstram que a segurança das cidades ainda é um desafio. As cidades adotam, de forma rápida, sistemas variados e complexos (ISMAGILOVA et al., 2019), mas parte das soluções abordam a segurança de forma específica para cada sistema, faltando uma visão global da cidade inteligente como um mosaico de sistemas interconectados (BRAUN et al., 2018). Essa

heterogeneidade facilita a exploração de vulnerabilidades, demandando que as soluções preventivas sejam adotadas de forma horizontal, envolvendo atores públicos, privados e a sociedade civil. Como muitos desses incidentes exploram o fator humano (engenharia social), entende-se que a prevenção deve envolver, além da tecnologia, os pilares social e político (BARTOLI et al., 2011).

Uma *smart city*, então, é composta por diversos pilares, que vão desde a implementação da tecnologia até a compreensão dessa por parte dos operadores e da sociedade civil. Esse excesso de camadas que compõem uma cidade inteligente permite uma variedade de ataques. Os principais riscos mapeados são: criação de mecanismos de vigilância, agregação de bases de dados, vazamento de informações, ataques a *hardware* ou infraestrutura, ataques a aplicações de cidades inteligentes, entre outros (NAUTIYAL; MALIK; AGARWAL, 2018).

Apesar da necessidade de uma visão global das lacunas de segurança, a maioria dessas se origina de vulnerabilidades técnicas dos dispositivos utilizados em *smart cities*. Essa infraestrutura variada faz com que as cidades inteligentes se tornem complexas demais para a gestão dos riscos de segurança, podendo deixá-las com uma estrutura frágil. Edwards (2016) alerta que a solução destes problemas, depois que as aplicações já estiverem implantadas, torna-se ainda mais difícil, pois atualizações ou *patches* já não são suficientes para resguardar uma arquitetura complexa. Isto pode levar estruturas de IoT a serem rapidamente inutilizadas, fenômeno que a autora denomina "*internet of junk"*.

Sendo assim, diante de um problema heterogêneo e da falta de uma abordagem unificada, fato é que a maioria dos projetos implementados se sustenta em uma frágil arquitetura de segurança, o que também pode prejudicar o tempo de resposta aos incidentes (THEODOROU; SKLAVOS, 2018). No que concerne às causas da vulnerabilidade das cidades inteligentes, destacam-se novamente a internet das coisas e o processamento de *big data* armazenado em nuvens digitais[20]. Em primeiro, a IoT é mais vulnerável que a computação tradicional, já que os

[20] Logicamente, não são somente estas tecnologias que compõem uma cidade inteligente, sendo estas somente as mais significativas dentre as que compõem o esqueleto urbano. Outra tecnologia de uso extremamente comum em serviços urbanos são os cartões inteligentes com *tags* baseados em RFID (identificação por radiofrequência). Esses *tags* podem ser utilizados para acionamento de serviços, registro de informações, dentre outras capacidades. Contudo, a simplicidade da tecnologia também é propensa à ocorrência de incidentes de segurança da informação (NAUTIYAL; MALIK; AGARWAL, 2018).

dispositivos possuem baixo poder computacional e dependem de sistemas simples que não comportam padrões elevados de segurança (QU et al., 2018).

Ademais, a proliferação de dispositivos aumenta a oportunidade de interceptação de comunicações entre estes. Edwards (2016) ressalta que a maioria dos aparelhos de IoT operam com base em comunicação sem fio e protocolos de encriptação fraca ou ausente. Para a autora, esses dispositivos são criados sem levar a segurança como prioridade, já que a garantia desta representa um desafio técnico. A isso se soma o fato de que os atacantes possuem capacidade crescente de explorar vulnerabilidades e de evitar a detecção, especialmente através de mecanismos de aprendizado de máquina (CUI et al., 2018).

Conforme explicado, o "*big data* urbano" é gerado por dispositivos de IoT, que enviam essas informações a servidores baseados em nuvens. Essa dinâmica de coleta e transmissão de *big data* também representa risco à segurança cibernética, produzindo oportunidades para a interceptação de dados. Theodorou e Sklavos (2018) alertam que a falta de ferramentas para lidar com bases de dados massivas, a ganância por dados e a transmissão contínua de informações aumentam o risco de incidentes. Ainda, os autores alertam que o setor público ainda não possui a expertise técnica para detectar nem para reagir aos citados incidentes, o que pode comprometer toda a infraestrutura de uma *smart city*.

Em resumo, existem diversos fatores que podem causar fragilidade na segurança dos dados nas cidades. Tanto a diversidade de sistemas como características intrínsecas a esses trazem desafios para a criação de um programa de segurança da informação sólido. Além disso, existem barreiras políticas e organizacionais, sendo difícil atribuir responsabilidades em arquiteturas complexas e dispersas através das cidades. Contudo, especialistas afirmam que, no momento, a maior barreira ainda é tecnológica (NAUTIYAL; MALIK; AGARWAL, 2018), já que os dispositivos utilizados ainda carecem da capacidade de resistir a ataques e a integração entre dispositivos heterogêneos é um desafio.

Sendo assim, as principais medidas a serem adotadas para a mitigação dos riscos dizem respeito à detecção das principais ameaças, das vulnerabilidades de cada tecnologia e dos desafios organizacionais. A garantia da segurança das informações é o primeiro passo para que o cidadão se sinta confortável em uma *smart city*, passando a interagir com a estrutura interconectada.

Ademais, além dos danos à segurança da cidade inteligente, especialistas em cibersegurança utilizam o bordão "*no privacy without security"* (ECKHOFF, WAGNER, 2018, p. 10). Ou seja, além de todos os efeitos colaterais que advém de um incidente de segurança, estes afetam o direito à privacidade e proteção de dados dos habitantes. Por isso, faz-se essencial a priorização da segurança informacional na fase de planejamento e implementação da tecnologia no tecido urbano. Se conseguirmos alocar de forma correta as obrigações e responsabilidades do Estado e das empresas fornecedoras, torna-se viável determinar quem deve abordar cada vulnerabilidade da cidade inteligente.

3.3. A Lei Geral de Proteção de Dados e as cidades inteligentes

Antes da Lei Geral de Proteção de Dados (LGPD), o tema da proteção de dados era tratado a partir de lentes mais privatistas, que consideravam a privacidade uma questão relacionada à intimidade da vida privada ou ao direito ao sigilo, como no caso do Código Civil de 2002[21] e da Constituição de 1988[22] [23].

As exceções à regra vieram através de legislações setoriais, como o Código de Defesa do Consumidor (Lei Federal nº 8.078 de 1990), a Lei do Cadastro Positivo (Lei Federal nº 12.414 de 2011) ou o Marco Civil da Internet (Lei Federal nº 12.965 de 2014), que previam alguns mecanismos de regulação do tratamento de dados pessoais, além de recursos para que o titular pudesse exercer direitos. O quadro se altera com a LGPD, que, assim como o GDPR, se insere na quarta geração de leis de proteção de dados. São normas que buscam garantir o direito à privacidade, a autodeterminação informativa e criar um aparato jurídico para a garantia desses direitos (DONEDA, 2019).

---

[21] Lei nº 10.406 de 2002. Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (BRASIL, 2002).

[22] CRFB, Art. 5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988)

[23] Ressalte-se que, no ano de 2020, o Supremo Tribunal Federal (STF), deu o primeiro passo para que o direito à proteção de dados seja entendido como um direito fundamental, sendo tutelado pelo regime constitucional e possuindo eficácia horizontal e direta sobre os temas relacionados à privacidade. A decisão foi tomada nos autos da ADI nº 6.387, que tratava sobre o uso de dados de geolocalização durante a pandemia do coronavírus (TORRES; AZEVEDO, 2020). Em sequência, no ano de 2021, o Congresso Nacional aprovou a PEC nº 17/2019, que inclui o direito fundamental à proteção de dados no texto da CRFB, além de instituir competência exclusiva da União para legislar sobre o tema.

A presença de um estruturado regime de proteção de dados brasileiro (DONEDA, 2020) é de primeira importância para o contexto das cidades inteligentes. A existência de um eixo central capaz de oferecer um regime jurídico completo para lidar com o tratamento de dados é essencial para que o tema possua segurança jurídica. Ainda, a adequação à LGPD é, hoje, uma demanda urgente para os setores público e privado, impactando diretamente na implementação ou contratação de serviços urbanos inteligentes.

Ademais, a submissão da proteção de dados a normas setoriais ou de caráter privatista deixaria lacunas imensas. Leis que tratem de aplicações específicas (como as relações de consumo ou provedores de internet) não são capazes de abarcar um fenômeno como as cidades inteligentes, que envolvem discussões que vão desde o fornecimento de energia até a participação política dos cidadãos. Ainda, uma visão privatista ligada à defesa negativa de um direito à não intromissão, seria insuficiente para reduzir a assimetria de poder entre o indivíduo e os agentes de tratamento de dados na cidade inteligente[24].

Por isso, em seus fundamentos (art. 2º[25]) LGPD vai além da defesa da intimidade, incluindo também a autodeterminação informativa, a defesa dos direitos humanos e o exercício da cidadania. O objetivo da lei é permitir que os titulares tenham a capacidade ativa de determinar como suas informações serão tratadas, além de posicionar a proteção de dados como uma questão intrínseca à participação na sociedade. Importante destacar que a LGPD não deve ser vista como uma barreira à inovação ou à cidade inteligente, visto que o desenvolvimento tecnológico e econômico também são fundamentos da norma. A lei deve ser vista

[24] Doneda (2019) entende que a privacidade se deslocou de um eixo ”pessoa-informação-segredo” para o eixo ”pessoa-informação-circulação-controle”. Não houve uma ruptura com a “privacidade original“, mas o centro de gravidade desta se reposicionou, somando novas características. Ou seja, o direito à privacidade se desloca de um conteúdo individualista para se tornar uma questão de natureza também coletiva, que incide na circulação da informação pela sociedade e garante ao cidadão o direito de controlar este fluxo.

[25] ”Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.” (BRASIL, 2018)

como guia para que a tecnologia seja implantada nas cidades de forma inovadora, sem permitir violações sistemáticas à privacidade.

Neste trabalho, não pretendemos exaurir a relação da LGPD com as cidades inteligentes, mas delinear os principais pontos de contato entre a norma e as cidades inteligentes contemporâneas, realizando análise de seus princípios e bases legais, da atuação do Estado e dos direitos garantidos aos titulares de dados. Ressalte-se, também, que uma abordagem mais concreta e prática sobre a aplicação da LGPD nas cidades será realizada no capítulo seguinte.

3.3.1. Princípios e direitos da LGPD nas *smart cities*

As novas leis de proteção de dados, como o GDPR e a LGPD, trazem um extenso rol de princípios que deve ser observado sempre que houver tratamento de dados pessoais, constituindo uma orientação obrigatória aos atores envolvidos. Os princípios marcam uma mudança cultural na abordagem dada aos dados pessoais, que era a de coletar o máximo possível de informações, sem muito critério ou transparência. Em linha com a valorização da autodeterminação informativa e do empoderamento dos titulares (VAINZOF, 2019), os princípios são parte essencial da última geração de normas de proteção de dados, fornecendo mecanismos para que os cidadãos sejam capazes de detectar formas abusivas ou ilícitas de tratamento de dados pessoais.

No presente capítulo, expusemos os principais desafios das cidades inteligentes quanto o respeito às leis de proteção de dados: (i) a coleta excessiva de dados pessoais; (ii) a dificuldade de atribuição de uma justificativa legal para todas as atividades de tratamento; (iii) a falta de transparência, para o cidadão, sobre o tratamento de dados; (iv) o risco de discriminação a partir de dados de baixa qualidade; (v) as potenciais vulnerabilidades de segurança da informação e (vi) a dificuldade de atribuição de responsabilidade nas atividades de tratamento (DONEDA; BELLI, 2021). Todas essas questões dizem respeito a princípios especificados pela LGPD, que serão abordados abaixo de forma breve junto aos direitos de titular aplicáveis.

3.3.1.1. Princípio da necessidade e anonimização de dados

Ao longo deste capítulo, expusemos que o uso de ferramentas como a IoT e a análise de *big data* trazem dificuldades relacionadas à coleta excessiva de dados pessoais. Estas tecnologias foram pensadas para coletar todos os dados possíveis e a sua interação com as normas de proteção de dados é ruidosa (DONEDA; BELLI, 2021). Não somente as cidades inteligentes coletam dados em massa, como ainda existe pouca transparência sobre os processos de descarte, o que torna real o risco de que estas grandes bases de dados sejam tratadas por períodos que vão além do necessário.

A coleta excessiva de dados é uma característica da economia movida a dados que vai muito além das cidades inteligentes e representa uma pedra fundamental da economia contemporânea (FRAZÃO, 2020). A partir da conclusão de que estas atividades possuem efeitos negativos, as legislações mais modernas, como a LGPD e o GDPR, adotaram o princípio da minimização. No Brasil, este foi nomeado princípio da necessidade, sendo definido pela LGPD (art. 6º, III) como: "*limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados*" (BRASIL, 2018).

Este princípio determina que os agentes de tratamento devem se limitar ao menor número possível de dados que permita a consecução da finalidade desejada. Isto também guarda relação com o período de conservação dessas informações, haja vista que a LGPD determina que o tratamento deve se encerrar tão logo atingida a finalidade ou o final do período de tratamento (VAINZOF, 2019). Ainda, é possível depreender deste princípio que a tecnologia adotada pelo controlador deve ser a menos intrusiva possível para o atingimento do objetivo, o que é um desafio nas cidades inteligentes (BREUER et al., s.d.).

Edwards (2016) argumenta que a interação entre *big data* e minimização é tensa, já que cientistas de dados tendem a buscar 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. Uma alteração nessa lógica demanda uma ampla reorientação de práticas de mercado consolidadas a partir da extração de *big data.* São essas práticas que penetram na cidade inteligente, em razão da dependência que estas possuem de tecnologia privada.

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.

Uma das principais formas de cumprir o princípio da necessidade é a partir da anonimização. Tal procedimento desnatura a caracterização da informação, fazendo-a deixar de ser considerada como dado pessoal perante a LGPD. O dado anonimizado é entendido pela lei como aquele "*relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*" (BRASIL, 2018). A LGPD autoriza os titulares a exigir a anonimização dos dados considerados desnecessários ou excessivos (art. 18, IV). Ou seja, o titular tem direito de exigir, do controlador, que este cumpra o princípio da necessidade.

Para Bruno Bioni (2020), o dado anonimizado é a antítese do dado pessoal, sendo aquela informação incapaz de identificar uma pessoa natural, que pode ser obtida através de procedimentos com variado grau de reversibilidade. Doneda e Machado (2019) argumentam que a anonimização é um fator essencial para que as cidades inteligentes sejam capazes de respeitar a proteção de dados, sendo estas obrigadas a anonimizar toda informação considerada excessiva. Tal prática abre novas possibilidades de pesquisa, negócio e desenvolvimento tecnológico nas *smart cities*, permitindo o compartilhamento de dados entre instituições com menor risco de violação à privacidade (KHAN; PERVEZ; ABBASI, 2017).

Contudo, uma dose de ceticismo é condição *sine qua non* para o uso responsável de técnicas de anonimização, já que nenhum processo pode ser considerado completamente irreversível e a maioria das tecnologias implementadas apresenta falhas (ECKHOFF; WAGNER, 2018). Não faltam exemplos de reidentificação, como no caso em que registros de 173 milhões de viagens de táxi feitas em Nova Iorque foram desanonimizados e vinculados a pessoas identificáveis no ano de 2013 (ANTONIALLI; KIRA, 2020).

A anonimização pode ser mobilizada por controladores que buscam se evadir da regulação das normas de proteção de dados, já que a LGPD não se aplica

às informações incapazes de identificarem uma pessoa natural. Desse modo, uma argumentação comum para o tratamento de *big data* é a alegação de que o conjunto não envolve dados pessoais, o que nem sempre é verdadeiro. Diante da dificuldade de efetiva anonimização, muitas das supostas bases anonimizadas contém informação pseudonimizada, que pode ser revertida para possibilitar a identificação de um indivíduo (EDWARDS, 2016).

De todo modo, ainda que a anonimização seja passível de críticas, esta não deve ser abandonada. Pelo contrário: deve ser um processo constante nas cidades inteligentes, pois diminui significativamente os riscos aos direitos dos titulares. Tais críticas são importantes para que, ao usar dados anonimizados, o administrador tenha consciência de que, apesar da redução do risco de violação de direitos, este ainda existe. Finch e Tene (2016) afirmam que, apesar de a anonimização não ser uma "bala de prata", ela possibilita o surgimento de oportunidades econômicas, de iniciativas de dados abertos e de recursos valiosos para a pesquisa e planejamento urbano.

Ainda, cabe mencionar que a anonimização é comumente categorizada como uma das principais tecnologias de potencialização da privacidade (*privacy enhancing technology* ou PET). Entretanto, as PETs vão muito além da anonimização, oferecendo ferramentas essenciais para a garantia da privacidade nas cidades inteligentes e tendo relação com o conceito de *privacy by design*. Este conceito, assim como as PETs, serão abordados no próximo capítulo.

Por fim, deve ser destacado que as autoridades deverão fiscalizar a relação entre as atividades de tratamento e o princípio da necessidade, podendo proferir sanções e determinar padrões mínimos a serem observados. A Agencia Española de Protección de Datos (AEPD) já proferiu diversas decisões sancionatórias em razão da violação do princípio da minimização nas cidades. O órgão estabeleceu que o uso de câmeras de vigilância por estabelecimentos privados deve observar o referido princípio, não podendo as câmeras estarem apontadas de forma contínua para espaços públicos. Em razão disso, a AEPD já proferiu sanções a estabelecimentos como bares, hotéis, casas de aposta e cafés cujas câmeras gravavam mais informações do que o necessário[26].

[26] Para consulta às decisões, consultar os seguintes processos: AEPD-PS/00389/2021, AEPD-PS/00427/2018, AEPD - PS/00369/2019 e AEPD - PS/00003/2020. As multas proferidas variam

3.3.1.2. Qualidade, não discriminação e decisões automatizadas

Anteriormente, mencionamos como a utilização de *big data* pode significar o uso de bases de dados de baixa qualidade, o que põe em risco a qualidade dos algoritmos de análise, podendo resultar em conclusões simplistas e até discriminatórias. Neste momento, analisaremos como esse fenômeno se relaciona com os princípios da qualidade e da não discriminação e com os direitos à correção de dados e à revisão de decisões automatizadas previstos LGPD.

Nas cidades inteligentes, o uso de *big data* não deve ser visto como inquestionável, já que depende da qualidade e do contexto dos dados tratados. Pesquisas demonstram, por exemplo, que dados de transporte urbano são ricos em volume, mas pecam na identificação da demografia que utiliza os serviços. Essas bases nos permitiriam conhecer as jornadas, mas não os indivíduos que estão em trânsito e, muito menos, as intenções destes. Mesmo assim, esses dados são considerados capazes de exaurir os fenômenos analisados, enquanto são somente amostras e representações deste (KITCHIN, 2020). Essa limitação não é um problema de volume, mas sim de qualidade de dados. Leia-se:

> Enquanto alguns argumentam que 'mais dados' é melhor do que 'dados melhores' e que o *big data* não necessita dos mesmos padrões de qualidade, veracidade e linhagem de dados pois a natureza exaustiva da base de dados remove vieses de amostra e compensa erros, lacunas e inconsistências no dado (Mayer-Schonberger and Cukier 2013), o fato é que ainda é verdade que a inserção de dados-lixo resulta em análise-lixo (KITCHIN, 2020, p. 47).[27]

Com atenção aos danos que podem ser causados pelo tratamento de dados de baixa qualidade, a LGPD consagrou o princípio da qualidade dos dados (art. 6º, V), que obriga os agentes de tratamento a garantir, aos titulares: "*exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento*" (BRASIL, 2018). Este comando

---

entre €1500 e €6000. Disponíveis para consulta em: https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub. Acesso em 2 de abril de 2022.

[27] "While some might argue that 'more trumps better' and that big data does not need the same standards of data quality, veracity, and lineage because the exhaustive nature of the dataset removes sampling biases and compensates for any errors or gaps or inconsistencies in the data (Mayer-Schonberger and Cukier 2013), it is still the case that garbage-data-in produces garbage-analysis-out". Tradução livre

demanda que os dados sejam precisos, relevantes e reflitam uma realidade atualizada, de modo a serem capazes de cumprir a finalidade listada.

O princípio da qualidade determina que os agentes de tratamento tenham responsabilidade no *input* de dados, o que é complementado pelo princípio da não discriminação, que veda a realização de tratamento discriminatório ilícito ou abusivo, objetivando impedir *outputs* que tratem os titulares de forma discriminatória (VAINZOF, 2019). A não discriminação guarda relação com a proliferação de vieses e resultados discriminatórios a partir de algoritmos de inteligência artificial defeituosos. Ou seja, a partir deste princípio, os agentes tornam-se responsáveis pelas práticas que adotam e tecnologias que utilizam, devendo agir para impedir resultados enviesados.

A redação da LGPD é relevante em um momento em que as cidades adotam tecnologias que impactam no cotidiano das pessoas. Tal fenômeno já é polêmico por si só, mas torna-se ainda mais grave quando dependente de dados de qualidade baixa (KITCHIN, 2020). Willis (2020) argumenta que as cidades inteligentes correm risco de institucionalizar vieses e de se tornarem incapazes de reconhecer realidades que fogem das conclusões obtidas através de dados. Confiando excessivamente em dados pouco confiáveis, a cidade poderá ignorar realidades complexas e, assim, excluir pessoas e comunidades de suas prioridades. Ou seja, decisões automatizadas enviesadas também tem um impacto negativo na democracia nas cidades (DONEDA; BELLI, 2021)

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 desse emaranhado pode ser um desafio. Entretanto, as cidades devem ser responsáveis, haja vista que as consequências dos resultados errôneos tem efeito direto nas vidas das pessoas, podendo determinar o redirecionamento de recursos públicos ou o rumo de políticas públicas relevantes (FINCH; TENE, 2016).

Para isso, é necessário entender como surgem as deficiências no *big data*, tarefa que deve ser realizada constantemente pelo corpo técnico das cidades inteligentes. Choenni et al. (2021) alertam que essas deficiências são praticamente impossíveis de serem totalmente sanadas, mas existem medidas que podem melhorar a qualidade dos dados. Em primeiro, os autores afirmam que diversas

bases de *big data* são formadas sem o contexto completo, ignorando categorias de dados que podem tornar a base de dados mais confiável. É uma missão complexa, já que significa na coleta de um volume maior de dados, mas a inclusão de dados faltantes pode dar um contexto mais preciso e evitar consequências negativas.

Ademais, deficiências na qualidade de dados advém principalmente do fato de que essas bases são geradas sem uma finalidade específica. 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 (CHOENNI et al., 2021).

Em terceiro, outra causa da baixa qualidade é a utilização de dados ou critérios de processamento defasados. Nas cidades, os ambientes estão em constante mudança, o que gera não somente novas informações, mas também novos contextos. Diante das mudanças, é possível que a cidade inteligente siga analisando dados que não mais refletem o presente. Ademais, ainda que a base de dados siga sendo atualizada, é possível que o contexto tenha se alterado a ponto de que os algoritmos utilizados se tornem incapazes de compreender a nova realidade (CHOENNI et al., 2021).

De modo que o titular de dados seja capaz de se opor à manutenção de dados de baixa qualidade pelo controlador, a LGPD prevê o direito à correção de dados incorretos, incompletos ou desatualizados (art. 18, III). Entretanto, o exercício de tal direito depende de transparência por parte do agente de tratamento e de conscientização por parte do titular. Neste sentido, é essencial a atuação por parte da ANPD, cujas atribuições incluem a fiscalização das práticas de tratamento e a auditoria dos agentes. A atuação proativa da ANPD é necessária para que a garantia de qualidade dos dados e de não discriminação não seja incumbência somente dos titulares, que se encontram em desequilíbrio de poder em relação aos agentes de tratamento (SOUZA; PERRONE; MAGRANI, 2021).

Além das medidas que objetivam aumentar a qualidade das bases de dados, outro fator é essencial para a realização do princípio da não discriminação: a possibilidade de revisão de decisões automatizadas (art. 20, LGPD). Este direito é uma ferramenta para potencialização dos princípios da qualidade e não discriminação, além de guardar intimidade com a transparência e o livre acesso,

relação que será explorada no item 4.4 ao abordarmos a efetivação da transparência algorítmica nas cidades inteligentes.

A consolidação global de um direito à revisão de decisões automatizadas se deu pelo fato de que, hoje, é possível que sistemas dotados de inteligência artificial atuem sem mediação humana, através da autoaprendizagem de máquinas. Nesse processo, "*o próprio sistema alcança resultados por meio de processos dedutivos e análises estatísticas que vão sendo determinados com base em correlações realizadas pela IA"* (MULHOLLAND; FRAJHOF, 2020, p. 268), o que permite que os padrões de decisão sejam impossíveis de se conhecer de forma prévia. Isto faz com que a suposta neutralidade e objetividade da tecnologia seja posta em xeque, estando os algoritmos sujeitos a erros e vieses.

O debate sobre a existência ou não de um direito à explicação perpassa pela previsão, em diversos contextos, de uma obrigação que os agentes de tratamento possuem de fornecer, aos titulares, informações sobre os processos de tomada automatizada de decisão adotados nas atividades de tratamento. Na Europa, o GDPR equipa o titular com o direito de acesso à informação diante da opacidade dos algoritmos, enquanto, em regra, proíbe o uso de decisões totalmente automatizadas. Por sua vez, a LGPD permite tais decisões, mas cria um amplo direito de revisão (SOUZA; PERRONE; MAGRANI, 2021).

A possibilidade de revisão de decisões automatizadas é uma condição essencial para a prevenção da discriminação nas cidades inteligentes. Mulholland e Frajhof (2020) argumentam que a conexão do direito à proteção de dados com a defesa dos direitos fundamentais evidencia que a revisão de decisões automatizadas é uma forma de se garantir o direito fundamental à igualdade.

É de se lamentar, contudo, a supressão da revisão humana do texto da LGPD, que acrescentaria mais uma camada de *accountability* ao processo. Entretanto, o veto proferido somente retira a obrigatoriedade de revisão por pessoa natural, não impedindo que esta venha a ser adotada como boa prática ou ser considerada como critério para que a revisão seja válida (SOUZA; PERRONE; MAGRANI, 2021). Nas cidades inteligentes, a promoção da confiança do cidadão é um passo essencial para a sustentabilidade dos projetos, o que certamente se beneficiaria da possibilidade de revisão humana.

As razões do veto à revisão humana alegam que tal processo inviabilizaria a inovação e os negócios das empresas, mas nem sempre isso é verdade, sendo o

processo de revisão uma possibilidade de geração de produtos mais qualificados. Mais do que uma forma de repressão da inovação nas cidades inteligentes, a revisão de decisões automatizadas deve ser vista como uma forma de obtenção de *feedbacks* oferecidos pelos titulares de dados, permitindo o aprimoramento da tecnologia utilizada (SOUZA; PERRONE; MAGRANI, 2021).

Quanto ao processo de revisão, a LGPD determina, em seu art. 20, §1º, que o controlador é obrigado a fornecer, quando solicitado, "*informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.*" (BRASIL, 2018). Quando não cumprir com tal obrigação, a ANPD é autorizada a realizar auditoria para verificar se há tratamento discriminatório. A presença desses mecanismos é importante para que não se sobrecarregue o titular, devendo a ANPD agir em situações de desequilíbrio de poder entre as partes, como nas cidades inteligentes.

Por fim, cabe mencionar que a ressalva aos segredos comercial e industrial é importante para que a garantia de direitos não seja um entrave para a inovação. O uso de sistemas protegidos por propriedade intelectual e industrial nas cidades inteligentes é inevitável e estes devem ter sua confidencialidade resguardada. Contudo, os controladores não podem se rejeitar a fornecer informações sob o escudo do segredo, o que legitima a atuação proativa da ANPD (MULHOLLAND; FRAJHOF, 2020). Nas *smart cities*, estes sistemas terão impacto sobre os cidadãos, devendo o segredo ser ponderado frente aos direitos humanos destes, justificando critérios mais rigorosos de auditoria ou então a adoção de sistemas de código aberto, temas que serão abordados no item 4.4.

3.3.1.3. Finalidade, adequação e bases legais

Os princípios da finalidade e adequação estabelecem que qualquer atividade de dados deverá ser realizada segundo uma hipótese prevista em lei e manter-se fiel, ao longo do tempo, às finalidades informadas ao titular de dados. Estes princípios impõem, aos controladores, a necessidade de uma justificativa específica para cada atividade de tratamento de dados, além de impedir que essas informações sejam reutilizadas de forma livre e injustificada (VAINZOF, 2019).

Isso demanda que o controlador seja capaz de atribuir uma base legal a cada atividade de tratamento. Na LGPD, tais bases legais são previstas pelos arts. 7º

(dados pessoais) e 11 (dados pessoais sensíveis), prevendo hipóteses específicas que autorizam tratar dados. Enquanto o princípio da finalidade limita o âmbito de ação dos controladores, obrigando-os a informar previamente a hipótese legal adotada, a adequação almeja garantir que o tratamento se mantenha compatível com a finalidade informada. Ambas as tarefas representam um desafio no contexto das cidades inteligentes, haja vista a larga escala de tratamento e a fluidez dos processos adotados (CHRISTOFI, s.d.).

Estes princípios viabilizam o princípio da necessidade, já que é após a atribuição das finalidades que se é possível determinar quais dados são essenciais para o atingi-las. Além disso, o princípio da adequação tende a cumprir papel relevante na cidade inteligente, já que previne a ocorrência do fenômeno de desvio de função[28] da tecnologia. Nas cidades, é comum que uma tecnologia seja implementada com uma finalidade original que se expande com o passar do tempo, pondo em risco os direitos dos titulares de dados (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.

O princípio da finalidade também demanda que os controladores adotem um grau de transparência em suas atividades de tratamento, devendo as finalidades serem comunicadas de forma clara e explícita. Nas cidades inteligentes, o cumprimento dessa obrigação requer o entendimento de que o público-alvo é amplo e envolve pessoas muitas vezes incapazes de entender a atividade de tratamento e a legislação de proteção de dados. Não podemos esquecer, também, que pessoas portadoras de deficiências também são objeto de atividades de tratamento, devendo ser contempladas pelo planejamento público. Ou seja, as administrações municipais tem o dever de utilizar linguagem acessível e didática, além de dar ampla divulgação aos seus projetos de cidade inteligente.

Conforme exposto, o Poder Público e as empresas envolvidas na cidade inteligente devem atribuir uma base legal às suas operações, o que pode ser uma tarefa difícil, em razão da dificuldade de obtenção de consentimento dos titulares e dos riscos atinentes à atribuição das outras bases legais aplicáveis. O consentimento é entendido pela LGPD como "*manifestação livre, informada e inequívoca*"

[28] Traduzido, livremente, do inglês "*function creep"* (CHRISTOFI, s.d.)

(BRASIL, 2018). Apesar de não ser uma base legal superior às outras, sendo todas igualmente válidas, o tratamento baseado no consentimento do titular se coaduna com o empoderamento dos indivíduos para realizar o controle de seus dados pessoais, que é o objetivo de leis como a LGPD e o GDPR.

Bioni (2021) afirma que estamos diante de uma dissonância entre norma e tecnologia, haja vista que a legislação se pauta na autodeterminação informacional dos sujeitos, enquanto as práticas de mercado tratam o titular como objeto de negócios pautados na extração vertical de dados. Nas cidades inteligentes, isso é evidente, tendo o titular pouca capacidade de realizar a gestão dos seus direitos e sendo a eficácia do consentimento posta em xeque (BREUER et al., s.d.).

Pesquisas realizadas em Bruxelas no ano de 2019 demonstraram que a retórica da viabilização do consentimento dos titulares na cidade inteligente, apesar de bem-intencionada, pode dar aos cidadãos uma falsa sensação de poder, diante da imensa dificuldade de coleta de um consentimento válido (CHRISTOFI, s.d.). Porém, nem sempre tal dificuldade se dá por opções de negócio e vigilância, podendo decorrer da estrutura tecnológica que sustenta a cidade inteligente.

O estabelecimento de um processo prévio e informado de coleta de consentimento vai contra a própria natureza da internet das coisas, pensada para se misturar ao ambiente em que coleta informações. Christofi (s.d.) relata que a IoT cria, nas *smart cities*, uma rede de sensores ubíqua e obscura, dificultando a viabilização de um consentimento lícito. Ainda, já expusemos que a coleta de *big data* costuma ser feita de forma indiscriminada e agregada, com definição posterior das formas de reutilização, o que dificulta estabelecimento de um consentimento prévio para finalidades específicas (EDWARDS, 2016).

A coleta de dados em espaços públicos também dificulta o consentimento livre. Estes espaços são destinados a serem usados pelos cidadãos 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 titular. 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.)

Lilian Edwards (2016), apesar de descrente na utilização do consentimento como base legal nas cidades inteligentes, fornece algumas sugestões como, por exemplo, a gravação de vídeos instrutivos para os cidadãos, o estabelecimento de

dashboards ou portais de gestão de direitos, a colocação de *QR codes* em dispositivos de IoT para acesso às políticas de privacidade ou a criação de ícones urbanos, como luzes, que sinalizam a coleta de dados. Porém, todos esses mecanismos são limitados, pois dependem da boa vontade do controlador, da disposição do titular e da sua capacidade de entendimento.

Logo, a realidade é que a maioria dos controladores optará por bases legais distintas do consentimento, que possui difícil constituição e requer gestão contínua da sua validade. 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 e capazes de violar direitos (EDWARDS, 2016).

Christofi (s.d.) ressalta que o GDPR permite o tratamento de dados para o atingimento de um interesse público ou de um interesse legítimo do controlador, o que autoriza os controladores a, mediante termos vagos, alegar a legalidade de suas operações. Mais do que isso, essas bases legais podem ser usadas, caso não haja fiscalização, para dar novas finalidades aos dados coletados. Este cenário impõe que os controladores sejam transparentes na atribuição de bases legais e sejam responsabilizados pelas consequências que causarem.

Na LGPD, o cenário é semelhante, existindo autorização para tratamento de dados para cumprimento de obrigação legal ou regulatória (art. 7º, II), para a execução de políticas públicas (art. 7º, III) e para atendimento dos interesses legítimos do controlador (art. 7º, IX). A tendência, nas cidades inteligentes, é que o Poder Público alegue a consecução de políticas públicas, enquanto o setor privado defenda a base legal do interesse legítimo (CHRISTOFI, s.d.). Ambas as bases legais requerem mecanismos de avaliação de impacto e da necessidade e proporcionalidade do tratamento, de modo a comprovar a sua adequação a uma política pública ou demonstrar que o interesse almejado é, de fato, legítimo.

Doneda e Belli (2021) argumentam, ainda, que as cidades inteligentes dependem de constante compartilhamento de informações pessoais entre entes públicos e privados, processo que ainda carece de uma base legal sedimentada. Por isso, estamos diante do risco de compartilhamento abusivo de dados nas cidades, faltando a criação de regras claras para que se cumpram os princípios da LGPD. Ainda, a elaboração de documentos regulatórios, como os relatórios de impacto à proteção de dados (RIPD) e o registro de operações de tratamento (RoPA), é um

processo essencial para evidenciar o cumprimento destes. Isto pois caberá à ANPD a verificação da licitude do tratamento nas cidades inteligentes, podendo requisitar tais documentos para avaliação da atividade de tratamento.

Cabe mencionar que a LGPD prevê diversos direitos que buscam empoderar o titular quanto à finalidade e adequação das operações de tratamento de dados. Sendo assim, o titular de dados tem direito de solicitar a eliminação dos dados tratados com o seu consentimento (art. 18, VI) e a eliminação de dados que forem tratados em violação à LGPD (art. 18, IV). No que diz respeito à validade deste consentimento, o titular possui o direito de exigir do controlador a informação sobre as consequências da negativa de consentimento (art. 18, VIII) e de revogar o consentimento previamente fornecido (art. 18, IX).

Contudo, o exercício desses direitos irá demandar que os atores da cidade inteligente forneçam informações claras e acessíveis sobre o tratamento que realizam e que possuam estrutura capaz de atender as demandas enviadas pelos titulares. Ainda, a efetivação do empoderamento pretendido pela LGPD depende de que os próprios titulares de dados tenham a iniciativa de tutelar seus direitos. Trata-se de situação desafiadora em contextos de desigualdade social e de dificuldade de compreensão dos projetos estabelecidos na cidade.

3.3.1.4. A transparência e o livre acesso

Diante da dificuldade de atribuição de base legal nas cidades inteligentes, talvez o melhor caminho seja promover a transparência para os cidadãos. 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).

O empoderamento do cidadão perante os agentes de tratamento é o resultado de um processo que tem suas origens na reação contra o monopólio das informações pelo Estado, que detinha vastos registros sobre a população, enquanto era pouquíssimo acessível a ela (BOURDIEU, 2014). Hoje, as demandas por transparência também se direcionam aos agentes privados, capazes de agregar quantidades massivas de dados com pouca claridade para os objetos dessa coleta.

Assim, na LGPD, estão presentes as orientações gerais para a efetivação da transparência e do acesso aos dados na cidade inteligente.

Segundo a LGPD, o princípio da transparência (art. 6º, VI) significa: "*garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*" (BRASIL, 2018). Este se relaciona com o do livre acesso (art. 6º, IV), que garante aos titulares o direito de consultar, de forma facilitada e gratuita, os seus dados, além de informações sobre a forma e duração do tratamento.

A concretização desses princípios depende do fornecimento de informações ao titular e a efetivação da transparência decorre de amplo acesso à informação, através do binômio transparência-informação (CHINELLATO; MORATO, 2021). Essas informações devem ser fornecidas de forma inequívoca e que privilegie a compreensão pelo cidadão médio (VAINZOF, 2019). Nas cidades inteligentes, então, a administração deve facilitar a experiência do titular, evitando a fadiga causada pela leitura de documentos excessivamente longos e técnicos.

Para viabilizar a efetivação destes princípios, a LGPD oferece um amplo ferramental de conceitos e direitos para os titulares. O art. 9º determina os critérios que devem ser observados pelos controladores ao garantir o acesso a dados, incluindo informações sobre finalidade, forma e duração do tratamento, a identificação do controlador, o compartilhamento de dados, as responsabilidades dos agentes e os direitos possuídos pelo titular. Essas informações devem ser fornecidas gratuita e ostensivamente em formato acessível e inteligível pelo público-alvo. Nas cidades inteligentes, podemos entender que os agentes de tratamento devem ser fiéis ao que exige a lei, tendo em vista a ampla variedade e incisividade das atividades de tratamento (FINCH; TENE, 2016).

A LGPD ainda prevê direitos ligados ao acesso e à transparência, os quais a cidade deverá estar preparada para atender. Em primeiro, o controlador deve, quando requisitado, confirmar a existência de tratamento (art. 18, I). Tal direito deve ser respeitado ainda que o titular tenha sido informado previamente do tratamento, permitindo a contínua gestão das operações (MALDONADO, 2019). Além da confirmação, o controlador deve fornecer o direito de acesso (art. 18, II) e informar sobre as consequências da negativa de consentimento (art. 18, VIII).

Para a transparência nas cidades, talvez o direito mais importante seja o previsto pelo art. 18, VII da LGPD, ou seja, o direito à "*informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados*" (BRASIL, 2018). A interação entre setor privado e Estado nas cidades inteligentes faz com que o cidadão tenha pouca visibilidade sobre o destino de seus dados (EDWARDS, 2016). Logo, a não concretização desse direito pode deslegitimar as operações perante a sociedade, devendo a cidade ser capaz de demonstrar quais dados troca com o setor privado (DONEDA; BELLI, 2021).

Em suma, a previsão destes direitos capacita o cidadão para exigir detalhes sobre o funcionamento da cidade inteligente. Novamente, é importante destacar que o titular não pode ficar sobrecarregado com estes pedidos. Ou seja, caso a ANPD detecte o tratamento de dados de forma pouco acessível e transparente, esta deverá agir para fiscalizar, avaliar e eventualmente sancionar os envolvidos.

Entretanto, apesar das normas mencionadas, a transparência é um conceito amplo, que permite diversas interpretações e possui variados desdobramentos na cidade. A efetivação desta depende de medidas que vão muito além da previsão de princípios e direitos em lei, sendo necessárias medidas concretas múltiplas, a exemplo dos citados mecanismos de revisão de decisão automatizada, das plataformas de acesso a dados públicos, da elaboração de documentos regulatórios e da estruturação de políticas e termos de uso para sistemas inteligentes.

A transparência deve ser pensada desde o início dos projetos de cidade inteligente (BREUER et al., s.d.), pois depende da nomeação de um encarregado de dados, da estruturação do atendimento aos titulares e de estratégias de conscientização e comunicação pública. Ainda, para que uma cidade inteligente seja transparente no tratamento de dados, essa deve ser capaz de conhecer seus processos, o que não é simples diante da dimensão e variedade de atividades de tratamento. Isso requer um refinado trabalho de mapeamento de dados e processos, além de uma estrutura principiológica capaz de orientar a cidade com relação aos processos mapeados (FINCH; TENE, 2018).

Em todas as acepções do conceito, a cidade inteligente depende de transparência e da confiança do cidadão, temas cuja concretização será explorada adiante. No presente capítulo foram delineados os princípios da transparência e do livre acesso, de modo a relacioná-los com as cidades inteligentes e com os direitos dos titulares, sendo reservada a sua aplicação concreta para o quarto capítulo.

3.3.1.5. Prevenção, segurança e responsabilização

Cidades inteligentes comportam de riscos de segurança da informação que se espalham entre o mundo digital e o espaço físico, trazendo novas facetas à discussão sobre cibersegurança. Com atenção à natureza de risco das atividades de tratamento, a LGPD estabelece princípios que obrigam os agentes de tratamento de dado a agir preventivamente e implementar medidas de segurança. Estes devem ser capazes de demonstrar a adoção dessas medidas e, caso estas sejam julgadas insuficientes, se responsabilizar pelas consequências adversas.

Este arcabouço é estruturado por três princípios estabelecidos no art. 6º da LGPD. O primeiro é o princípio da prevenção (inciso VII), que impõe a "*adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*" (BRASIL, 2018). Com relação às cidades inteligentes, sua implementação tem relação com a forma com que se planejam os projetos de serviços inteligentes. Em regra, a proteção de dados não é um fator de destaque no planejamento, sendo vista como um empecilho, o que dificulta a sua inserção na fase de *design* do projeto. Ainda, a prevenção torna-se mais difícil pela maioria das cidades inteligentes ser construída de pouco em pouco em uma malha urbana já existente, o que dificulta a medição dos riscos entre diversos fornecedores.

Uma forma de se observar o princípio da prevenção é a elaboração de relatórios de impacto à proteção de dados (RIPD) (CHRISTOFI, s.d.), documentos regulatórios pensados para o mapeamento e mitigação dos riscos de atividades de tratamento. O RIPD, previsto pelo art. 5º, XVII da LGPD, deve ser elaborado quando houver risco de violação de direitos fundamentais decorrente da atividade de tratamento, sendo obrigatório para serviços de cidades inteligentes, cujo impacto atinge um grande volume de titulares. No capítulo seguinte, será discutido como inserir o RIPD na lógica de construção de *smart cities*.

Já o princípio da segurança determina a adoção de medidas técnicas e administrativas para a prevenção de incidentes de segurança. As medidas técnicas são aquelas ligadas à tecnologia da informação e ciência da computação, como *firewalls*, recursos de controle de tráfego, criptografia, entre outros. Por sua vez, medidas administrativas envolvem o fator gerencial e jurídico da segurança,

dependendo da elaboração de políticas, da promoção de treinamentos, da adequação de contratos, entre outras medidas (JIMENE, 2019).

Em razão do grande número de titulares envolvidos, do volume expressivo de dados tratados e da interação entre o espaço cibernético e o espaço físico, Doneda e Machado (2019) entendem que a garantia de segurança da informação é uma prioridade para as cidades. Trata-se de um desafio, já que, conforme mencionado, os sistemas de cidade inteligente são adotados de forma progressiva e heterogênea, havendo pouca clareza sobre os riscos e atores envolvidos. Os autores destacam que, nos últimos anos, municípios brasileiros adotaram serviços inteligentes antes da entrada em vigor da LGPD, obedecendo somente requisitos da legislação municipal apesar de já existirem normas como o Marco Civil da Internet, que impunham padrões mais rigorosos de segurança.

Breuer et al. (s.d.) ressaltam que a garantia do princípio da segurança nas cidades inteligentes requer, ainda, monitoramento contínuo dos sistemas implementados. Isto porque a tecnologia evolui ao longo dos projetos urbanos, podendo ser direcionada para novos usos ou até ser substituída por novas tecnologias. Essas mudanças impactam nos riscos diagnosticados, o que demanda novas abordagens e medidas de segurança informacional.

Ainda, ao diagnosticar os riscos na cidade inteligente, os controladores devem assumir a obrigação de mapear riscos concretos e adequados à realidade local, sob risco de que a auto-avaliação torne-se um processo mecânico e formalístico. Nas palavras de Breuer et al., a avaliação de riscos não pode ser um "processo de marcar caixinhas"[29] excessivamente baseado em documentos. Por isso, a administração pública e os agentes privados devem ser capazes de entender as expectativas do cidadão impactado pela tecnologia, de modo a avaliar como cada aplicação afetará cada grupo.

Por último, o princípio da responsabilização e prestação de contas (art. 6º, X) determina que os agentes de tratamento sejam capazes de demonstrar a: "*adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*" (BRASIL, 2018). A necessidade de responsabilização de agentes de tratamento advém da conclusão de que tratar dados pessoais possui efeitos sobre os direitos

[29] "There is a threat that accountability will be seen by controllers as a box-ticking exercise". Tradução livre.

das pessoas (SCHREIBER, 2021), podendo causar dano moral ou patrimonial aos titulares de dados.

Neste sentido, a LGPD determina que uma atividade de processamento de dados será irregular se for incapaz de garantir a segurança do titular ou quando violar a legislação, devendo ser avaliados: o modo de tratamento, o resultado, os riscos avaliados e as técnicas de tratamento disponíveis à época (BRASIL, 2018). Uma das formas mais evidentes de violação de direitos é a ocorrência de incidentes de segurança, infrações listadas pelo art. 46 da LGPD e que devem ser entendidas como violações das medidas de segurança implementadas pelos agentes de tratamento (SOUZA, 2020).

Dificilmente, um incidente de segurança irá afetar somente um titular de dados, já que as bases de dados costumam ser amplas. Nas cidades inteligentes, a ocorrência de incidentes de segurança possui evidente natureza coletiva, podendo impactar números significativos de habitantes cujos dados foram coletados. Neste contexto, é importante a previsão, pela LGPD, de instrumentos coletivos para tutela de direitos (art. 42, §3º). Diante de um incidente em uma cidade inteligente, a possibilidade de ajuizamento de uma única ação por todos os afetados (SCHREIBER, 2021) é mecanismo essencial para a responsabilização.

Quanto ao regime de responsabilidade civil aplicável às violações à LGPD, trata-se de, talvez, o assunto mais debatido entre especialistas em proteção de dados. A exaustão desse tema exacerba o escopo desta pesquisa, dependendo de aprofundada análise dos regimes subjetivo e objetivo de responsabilidade. Schreiber (2021) entende que não existe resposta unívoca, na LGPD, para a definição de um regime de responsabilidade, já que a norma prevê violações que dependem da conduta do agente e define ocasiões em que a norma segue uma avaliação baseada no risco da atividade, comum à responsabilidade objetiva.

Entretanto, apesar da necessidade de análise casuística, é provável que a maioria dos incidentes de segurança e violações aos direitos de proteção de dados nas cidades inteligentes ensejem responsabilidade civil objetiva, que independe da aferição de culpa. Isto pois a prestação de serviços públicos é abordada a partir da teoria do risco administrativo, exigindo somente a configuração da conduta, do dano e do nexo causal entre estes (art. 37, §6, CRFB). O mesmo se aplicará às empresas contratadas para a prestação de serviços nas cidades inteligentes, haja

vista a aplicação da teoria do risco às concessionárias de serviços públicos, entendimento sedimentado pela legislação e pela jurisprudência.

Ainda, importante mencionar que a atribuição de responsabilidade nas *smart cities* pode ser um processo difícil a depender da transparência do projeto. Cidades inteligentes são uma combinação de projetos que dependem de empresas de tecnologia e se espraiam por diversas áreas do Estado (BREUER et al., s.d.). Neste contexto, pode ser pouco claro quem deve ser entendido como responsável, o que torna relevante a previsão, pela LGPD, de hipóteses de responsabilidade solidária em caso de violação das instruções do controlador pelo operador (art. 42, §1º, I) e em caso de controladoria conjunta (art. 42, §1º, II).

Por fim, agentes de tratamento são fiscalizados e podem ser eventualmente responsabilizados por parte da ANPD. Por isso, a LGPD garante que os titulares possuem direito de peticionar ao órgão caso considerem que seus direitos foram violados (art. 18, §1º). Tal direito foi regulamentado pela ANPD em 2021, quando o órgão estabeleceu sistema de peticionamento para titulares. A ANPD somente aprecia petições apresentadas e não solucionadas pelos controladores, o que impõe que as cidades possuam estrutura administrativa para apreciação de pedidos de titulares de dados, sob pena de sancionamento pela Autoridade.

3.3.2. O Poder Público enquanto agente de tratamento

Conforme exposto, grande parte da construção teórica dos direitos à privacidade e proteção de dados busca impedir a intromissão indesejada e o abuso de poder por parte do Estado. Por mais que a proteção de dados tenha evoluído de um direito meramente negativo para o empoderamento dos cidadãos, a sua origem não foi esquecida, sendo o excesso de vigilância estatal ainda uma preocupação premente do direito contemporâneo.

Diante de um Estado com capacidades exageradas para tratamento de dados de forma abusiva ou pouco transparente, há risco concreto de violações de direitos fundamentais de primeira geração (como a liberdade) e de quarta geração, relacionados aos direitos humanos na sociedade da informação (XAVIER, L. P.; XAVIER, M. P.; SPALER, 2020). Sendo assim, é necessário que se aplique, ao Poder Público, um regime que busque regular as suas atividades de tratamento, sendo este o objetivo do "Capítulo IV" (artigos 23 a 32) da LGPD.

Ainda, nas cidades inteligentes, é frequente a contratação de agentes privados para a prestação de serviços públicos, seja no formato de concessões, parcerias público-privadas (PPP) ou no fornecimento de tecnologia e expertise ao Estado. Em razão disso, faz-se necessária, também, a regulação do compartilhamento de dados pessoais dos cidadãos entre o Estado e atores privados, o que é, apesar de graves lacunas, abordado pela LGPD.

Para delimitar o âmbito de ação do Poder Público, a LGPD, em seu art. 23, estabelece que o tratamento de dados pessoais realizado por pessoas jurídicas de direito público deverá objetivar a consecução de finalidade pública ou interesse público, sempre em cumprimento de suas competências ou atribuições legais. Ainda, a lei estabelece condições: a publicação, em veículos de fácil acesso, de informações claras sobre as operações de tratamento realizadas (inciso I) e a indicação de um encarregado de dados (inciso III).

Neste ponto, argumenta-se que a submissão de qualquer operação de tratamento de dados ao requisito de cumprimento do "interesse público" é demasiadamente vaga, podendo significar uma perda de efetividade por parte da lei (XAVIER, L. P.; XAVIER, M. P.; SPALER, 2020). Isto ocorre pois ainda não temos como avaliar a forma com que a Administração Pública se vincula aos princípios da finalidade e adequação, faltando transparência às suas atividades de tratamento. Ademais, o conceito de interesse público é um dos mais contenciosos do direito, podendo ter incidência menor ou maior a depender do contexto, o que acaba por deixar à mercê do administrador a sua definição.

Nas cidades, a maior preocupação diz respeito ao compartilhamento de dados entre agentes públicos e privados. A LGPD (art. 26, §1º) determina que o Poder Público poderá compartilhar dados com agentes privados em diversas hipóteses, como a execução descentralizada de atividade pública, quando o compartilhamento for baseado na execução de contratos ou convênios ou para fins de prevenção à fraude e garantia da segurança do titular. Tal artigo abre diversas brechas para o compartilhamento com atores privados engajados na prestação de serviços públicos. Como exposto, os titulares têm pouca visibilidade sobre como esses dados são compartilhados ou sobre como exercer seus direitos, já que não é claro quem é o controlador de dados da *smart city*.

Ainda, ao que parece, a LGPD adiciona vedações ao Estado que não se sustentam diante das próprias exceções criadas pela lei. Ao mesmo tempo que a

norma condiciona o compartilhamento de dados a agentes privados ao consentimento do titular (art. 27, III), ela permite que o consentimento seja derrogado diante das exceções previstas no art. 26, §1º, que abarcam praticamente a totalidade dos projetos de *smart city,* facilmente vinculáveis ao interesse público ou à execução de política pública.

Não se trata de defender que o compartilhamento seja proibido, já que isto significaria a inviabilização completa do exercício de políticas públicas e o cancelamento do projeto de cidade inteligente. É certo que tais consequências não são desejadas e vão manifestamente contra os fundamentos da LGPD. Por isso, Doneda e Belli (2021) argumentam que as cidades inteligentes se beneficiariam da existência de uma base legal específica para o compartilhamento entre entes públicos e privados. Ainda, existem meios, que serão abordados no próximo capítulo, para garantir maior transparência e estimular que os agentes envolvidos em tais operações de compartilhamento tenham maior responsabilidade.

Entretanto, 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). Se já existe a preocupação do compartilhamento de dados pessoais ordinários com o setor privado, o compartilhamento de dados relacionados às atividades repressivas é sensível, diante da não incidência da LGPD (MENEZES; COLAÇO, 2020).

Não faltam exemplos, no Brasil, de projetos de cooperação entre o Estado e as empresas com finalidades de segurança pública, como o uso de reconhecimento facial em estádios de futebol ou o programa *City Camera*, promovido pelo município de São Paulo, com a finalidade de receber imagens captadas por câmeras privadas para fins de segurança (ABREU, 2021). Estes projetos são, aliás, parte integrante de muitos projetos de cidade inteligente, a partir de tecnologias como o policiamento preditivo e o reconhecimento facial.

A criação de sistemas abusivos de policiamento inteligente nas cidades é ainda mais preocupante em países desiguais, como o Brasil, marcados pela violência policial que atinge desproporcionalmente grupos minoritários, como a população negra e pobre. Tais projetos de policiamento inteligente ainda são enviesados, podendo reproduzir o racismo existente na sociedade.

Segundo Samuel de Oliveira (2021, p. 75), a utilização de estatísticas probabilísticas para a previsão de crimes opera em uma lógica circular: "*a produção de estatísticas oficiais também é baseada em hipóteses preconcebidas sobre como se dá a prática da criminalidade, o que, por si só leva a ações policiais – formais e informais – de caráter discriminatório".* A mesma crítica pode ser feita a sistemas de reconhecimento facial[30] que forem alimentados por dados enviesados ou dependentes de algoritmos imprecisos. Oliveira ressalta que estes sistemas produzem um número expressivamente maior de identificações incorretas quando tratam dados da população negra, exacerbando, através da tecnologia, a discriminação já existente na sociedade.

A não incidência da LGPD pode representar barreira para que os cidadãos exerçam seu direito de revisão às decisões automatizadas tomadas por sistemas inteligentes de policiamento, o que aumenta o risco de violações de direitos. Menezes e Colaço (2020) alertam que a não submissão dessas atividades à LGPD deixa dúvidas sobre a competência da ANPD para fiscalização dessas operações de tratamento, havendo uma significativa lacuna regulatória.

Entretanto, o regime da LGPD para a segurança pública não é uma carta branca, já que a norma menciona que essas operações de tratamento ainda devem ser submetidas aos limites da Constituição Federal e da legislação, além de observarem os princípios gerais da LGPD (ABREU, 2021). A norma também determina, para reduzir o protagonismo do setor privado na segurança pública, que nenhum banco de dados utilizado para essa finalidade poderá ser de controle integral de empresas privadas (art. 4º, §4º) e que a ANPD deverá ser informada da participação dessas em tratamento de dados para fins de segurança (art. 4º, §2º).

Em conclusão, a participação do Estado e das empresas enquanto agentes de tratamento ainda depende de regulação mais aprofundada. No caso da segurança pública, existe a previsão expressa de que o tema deverá ser tratado por lei específica, que ainda não existe. Entretanto, no que diz respeito aos projetos de *smart city* em um contexto amplo, cabe a regulação por parte da ANPD, que possui competência (art. 30, LGPD) para estabelecer normas complementares para reger o

[30] No dia 22 de março de 2022, a justiça estadual de São Paulo proferiu decisão liminar em ação civil pública para proibir a instalação de sistemas de reconhecimento facial no sistema metroviário do estado. Em sua decisão, a juíza afirma que o sistema seria implantado de forma abusiva e pouco transparente, devendo ser vetada até a comprovação da resolução das deficiências técnicas do sistema (SÃO PAULO, 2022).

compartilhamento de dados entre o Estado e o setor privado. Trata-se de oportunidade para que a Autoridade publique regramento contendo obrigações e requisitos para o desenvolvimento da cidade inteligente.

3.4. A Carta Brasileira para Cidades Inteligentes

Diante de novas tecnologias, é comum a elaboração de estratégias nacionais para a aplicação destas. É neste contexto que foi elaborada a Carta Brasileira para Cidades Inteligentes (CBCI), que define objetivos e diretrizes do país para *smart cities.* O documento foi produzido em sequência à publicação do Plano Nacional de Internet das Coisas (Decreto nº 9.854 de 2019), que define conceitos e estabelece objetivos para a utilização da IoT no Brasil.

Ao contrário do Plano Nacional de IoT, a CBCI não possui força de lei, sendo uma declaração de intenções elaborada pelo Ministério do Desenvolvimento Regional, com apoio das Secretarias de Mobilidade, Desenvolvimento Regional e Urbano e de Telecomunicações do Ministério de Ciência, Tecnologia, Inovações e Comunicações. Também participaram de sua elaboração outros atores públicos e privados, sendo o documento resultado de metas do PNUD - Plano Nacional de Desenvolvimento Urbano (LAPCHENSK; FERREIRA; CASTAGNA, 2021).

A CBCI trata da cidade inteligente como um todo, estabelecendo uma definição, já mencionada, para o conceito. Em suma, a Carta Brasileira determina as principais metas para um desenvolvimento urbano sustentável e inteligente, abordando as mais diversas áreas do urbanismo. Não cabe, neste momento, uma exploração aprofundada da CBCI, mas sim dos pontos em que o documento toca no tema da proteção de dados pessoais e privacidade.

A elaboração da CBCI demonstra a necessidade de diálogo entre as partes envolvidas nos projetos de cidade inteligente (BARBOSA; COSTA; PONTES, 2020), envolvendo tanto autoridades federais quanto locais e mobilizando também atores do setor privado. A Carta se insere no contexto da Nova Agenda Urbana (NAU), definida em 2016 nas Nações Unidas, com objetivo de determinar as diretrizes do urbanismo para os próximos vinte anos. O *Issue Paper 21 – Smart Cities*, produzido no âmbito da NAU, dá destaque à cidade inteligente, com atenção às potencialidades e contradições deste modelo urbano (REIA, 2019).

Jhessica Reia (2019) afirma que o resultado da NAU é interessante sob diversos pontos, mas que a ausência do debate sobre proteção de dados nas cidades é uma grave deficiência. Nesse sentido, a ONU Habitat segue a linha da maioria das estratégias nacionais, excessivamente focada em questões ambientais e econômicas, abordando a proteção dos dados pessoais de forma breve. Por sua vez, a CBCI surpreende positivamente, indo além da NAU e da maioria das cartas compromisso sobre *smart cities*.

A Carta adota oito objetivos estratégicos, ressaltando que a relação entre estes objetivos é simbiótica, ou seja, que estes são interdependentes e que a não consecução de um destes põe os outros em prejuízo. Estes objetivos se reúnem sob o objetivo amplo de "*transformação digital sustentável*", envolvendo tanto temas quanto desigualdade social e responsabilidade ambiental como a privacidade e proteção de dados (BRASIL, 2019). Dentre esses, se insere o Objetivo Estratégico 3:

> Estabelecer sistemas de governança de dados e de tecnologias, com transparência, segurança e privacidade
> **Contexto ›** *Políticas públicas e conectividade são elementos básicos, mas insuficientes para equidade (distribuição justa, capaz de atender necessidades diferentes de todas as pessoas) de oportunidades no contexto da transformação digital. É preciso estruturar sistemas de governança de dados e de TICs (tecnologias de informação e comunicação) adequados a cada realidade. Somente a partir desses sistemas será possível integrar infraestrutura, sistemas, ferramentas e soluções digitais no desenvolvimento urbano de todas as cidades.*
> Diferentes governos e setores da sociedade devem cooperar para os sistemas funcionarem de forma integrada, responsável e inovadora. Com segurança cibernética e garantia de privacidade pessoal. Devem cooperar para oferecer um ambiente de ética digital que assegure dados compartilhados e abertos sempre que possível e que garanta proteção jurídica às pessoas (BRASIL, 2019, p. 33).

Ao desenvolver o Objetivo Estratégico 3, a CBCI demonstra estar ciente da maioria dos problemas relatados neste capítulo, estabelecendo nove recomendações para a promoção da governança de dados e proteção da privacidade nas cidades inteligentes. Dentre elas, se destacam: a garantia da segurança cibernética, a adequação à LGPD, a promoção da transparência algorítmica, a criação de padrões de interoperabilidade entre sistemas, a criação de políticas de dados abertos e a promoção do governo digital (BRASIL, 2019).

Indo além da mera listagem de objetivos, a CBCI fornece exemplos de como atingi-los, além de elencar quais atores são responsáveis pela efetivação destes. Ou

seja, a Carta dedica atenção ao fato de que a cidade inteligente é um esforço conjunto, que depende de um fino ajuste entre diversas instâncias. Infelizmente, o documento somente serve como uma declaração de intenções, sem força normativa para que sua implementação seja demandada oficialmente. Ainda assim, a sua publicação representa um norte para uma cidade inteligente brasileira capaz de atingir seus objetivos sem desrespeitar a privacidade dos seus cidadãos.

4. Como equacionar “inteligência” e privacidade?

Um dos principais desafios contemporâneos na regulação da tecnologia é a dificuldade de comunicação e a disputa por protagonismo entre aqueles que propõem soluções na esfera jurídica e os que oferecem soluções técnicas para os defeitos de cada nova tecnologia. A cidade é matéria de muitas facetas, que pode ser abordada a partir de diversos prismas que, muitas vezes, entram em conflito. Nas cidades inteligentes, tal problema é evidente: sobre o assunto, debruçam-se engenheiros, urbanistas, geógrafos, sociólogos, juristas e uma série de atores.

A experiência já nos demonstra que esta falta de diálogo gera ineficiência, haja vista que uma solução tecnológica que não se coadune com os limites jurídicos será inútil, assim como uma regulação ousada pode ser de implementação tecnologicamente inviável. Dessa forma, a única maneira eficiente de minimizar os danos à privacidade na *smart city* é combinar soluções de ordem jurídica e tecnológica, objetivando criar um arcabouço legal capaz de prevenir e reagir a danos e uma cultura de proteção de dados, sem que isto signifique uma barreira à inovação e ao desenvolvimento (FINCH; TENE, 2016).

Este capítulo objetiva expor, de forma não exaustiva, algumas ferramentas do direito e da tecnologia que podem e devem ser adotadas nas cidades do futuro.

4.1. Implementando a LGPD nas cidades

A implantação e fiscalização de normas de proteção de dados é um dos principais desafios jurídicos contemporâneos, haja vista a rápida evolução da tecnologia, a multiplicidade de atores envolvidos e a complexidade da regulação. No contexto das cidades, esta dificuldade se exacerba, já que estão envolvidos atores públicos e privados e o tratamento de dados pessoais ocorre em larga escala, comportando diversos riscos.

Ainda não há estudo sistemático sobre os desafios de implantação da LGPD nas cidades inteligentes, mas é possível realizar, diante da proximidade das normas, uma comparação com o GDPR. Segundo Breuer et al. (s. d.), as cidades inteligentes representam um desafio para a legislação europeia de proteção de dados pois: (i) envolvem uma variedade de riscos de violações a direitos fundamentais; (ii) geram

uma dificuldade de avaliação de riscos e efeitos danosos em razão das diversas camadas e atores envolvidos; (iii) o engajamento dos cidadãos é limitado, assim como a transparência das iniciativas e (iv) a participação de agentes privados reduz o controle sobre o tratamento de dados.

Diante disso, duas medidas parecem essenciais para a implementação de um programa de privacidade e governança de dados nas cidades, quais sejam, a nomeação de um Encarregado de dados (DPO) e a elaboração de documentos regulatórios, como o RIPD e o registro de atividades de tratamento.

4.1.1. Encarregado de dados

A função de encarregado de dados, prevista na LGPD, é equivalente à figura do *data protection officer* previsto pelo GDPR e comumente chamado de DPO. 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). Sua indicação é obrigatória para todos os controladores[31], sendo as atividades previstas pela LGPD:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018).

Ou seja, em linhas gerais, o encarregado é o ponto de contato entre o controlador, as autoridades e os titulares de dados, servindo para gerenciar internamente os projetos de *compliance* à legislação de proteção de dados e para interagir com as solicitações direcionadas ao controlador.

[31] Recentemente, a ANPD publicou norma que dispensa agentes de pequeno porte da nomeação de DPO. Contudo, no contexto das cidades inteligentes, não há que se falar em agente de pequeno porte, já que a incidência das operações de tratamento é amplíssima e as atividades de tratamento costumam representar risco de violação de direitos fundamentais. A norma publicada pela ANPD determina que não poderão ser considerados agentes de pequeno porte aqueles que realizarem tratamento de alto risco, o que inclui: tratamento em larga escala, tratamento de dados que possam afetar direitos fundamentais, uso de tecnologias inovadoras, vigilância de zonas públicas, decisões automatizadas, entre outros (BRASIL, 2022). Logo, resta claro que a consideração de qualquer ator envolvido em projeto de cidade inteligente como agente de pequeno porte faz-se inviável.

No contexto das cidades inteligentes, a LGPD prevê que o Poder Público deverá nomear encarregado quando realizar operações de tratamento de dados (art. 23, III). Indo além, existem pesquisas e projetos no sentido de que, além da nomeação de encarregados específicos dentro de órgãos ou projetos públicos, seja nomeado um agente para atuar como encarregado no âmbito do município. Tal solução pode ser uma eficiente maneira de reduzir a opacidade das formas de tratamento e armazenamento 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.

Buscando delimitar o papel e as funções do encarregado, a ANPD publicou, em 2022, processo de tomada de subsídios, no qual busca coletar opiniões da sociedade civil, da pesquisa e do setor privado. Dentre os cinco blocos de perguntas elencados pela Autoridade, o 'Bloco 5' busca coletar subsídios sobre a nomeação do encarregado no setor público, o que tende a influenciar diretamente nos projetos de cidade inteligente. Existem, ainda, perguntas que tratam especificamente sobre a nomeação de encarregado municipal. Leia-se:

> 9) Qual seu ponto de vista quanto à dispensa ou flexibilização da designação do encarregado por municípios? No caso positivo, quais seriam os critérios? Haveria outras hipóteses de dispensa ou flexibilização da designação do encarregado no setor público?
> 10) Ainda relativamente aos municípios, é possível a indicação de um único encarregado por mais de um município? Em caso afirmativo, em que circunstâncias? Quais medidas devem ser observadas? (ANPD, 2022)

O processo ainda não foi concluído no momento desta pesquisa, mas as perguntas listadas são preocupantes com relação às cidades inteligentes. A posição de encarregado deve ser entendida como essencial para os municípios brasileiros diante do crescente uso de tecnologia no tecido urbano, sendo temerário pensar em hipóteses de dispensa de nomeação. Ainda, a nomeação do mesmo encarregado por mais de um município pode agravar o problema de que as cidades inteligentes são construídas de forma universalista, já que um encarregado que não conhece a cidade pode não ser capaz de avaliar a necessidade e proporcionalidade do tratamento de dados.

No exterior, as cidades parecem caminhar pelo sentido oposto. 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 uma estrutura composta por especialistas. Nos EUA, a figura do encarregado (DPO) 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 e conscientização. Além do CDO e do CPO, cidades americanas tem adotado outras posições, como o *chief innovation officer* e o *chief technology officer*, respectivamente 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, por exemplo, 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 entre 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).

Apesar de a posição indiana priorizar profissionais do ramo da tecnologia, a função do CDO é muito semelhante à do encarregado previsto pela LGPD, sendo também responsável pelo processamento de solicitações de titulares de dados e da promoção de uma cultura de proteção de dados nas cidades. O CDO é o responsável por garantir que os dados gerados por uma cidade sejam usados de forma correta, além de servirem como um ponto único de contato para o tema. Por fim, ressalta-se que o CDO se submete à administração municipal, mas espera-se que essa lhe

garanta a independência necessária para que o programa de governança de dados tenha sucesso (GOVERNMENT OF INDIA, 2018).

No Brasil, ainda não há nenhuma movimentação por parte do Congresso Nacional ou da ANPD para a instituição de uma figura semelhante ao CDO, o que seria uma adição relevante para as cidades inteligentes brasileiras.

Apesar disso, algumas iniciativas locais merecem destaque, como a Lei Ordinária nº 7.012 de 2021 do Município do Rio de Janeiro, que instituiu o Conselho Municipal de Proteção de Dados e da Privacidade, composto por integrantes da Prefeitura, da Câmara de Vereadores, da sociedade civil e do setor privado. 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, promovendo eventos e estudos, além de possuir responsabilidade de promover a cultura de proteção de dados junto à população do município do Rio de Janeiro.

Ainda que o Conselho não possua capacidade[32] de atuar como ponto de interação com os titulares de dados e de estabelecer diretrizes obrigatórias para projetos de cidades inteligentes, o órgão possui estrutura de auxiliar a Administração Pública. Ademais, 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*.

4.1.2. Relatório de Impacto à Proteção de Dados (RIPD) e Registro de Operações de Tratamento (RoPA)

Uma das principais características da legislação adotada no Brasil, sob influência do GDPR europeu, 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

[32] Importante ressaltar que existe dúvida quanto à constitucionalidade de projetos locais como esse, em razão da inclusão da competência privativa da União para legislar sobre temas de proteção de dados na Constituição. A alteração foi feita pela Emenda Constitucional nº 115/2022, que determinou que cabe à União organizar e fiscalizar a proteção de dados pessoais e legislar sobre o tema. Entretanto, entendemos que a norma constitucional não proíbe que os municípios se organizem, desde que essa organização não esbarre na competência privativa da União e siga as normas de proteção de dados em sua integralidade. Para isso, seria benéfica a emissão de diretrizes por parte do Executivo Federal, delimitando até onde podem ir os municípios no exercício de suas atribuições.

de Dados (RIPD), uma adaptação nacional do *Data Protection Impact Assessment* (DPIA), 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).

As análises de impacto já existiam no direito brasileiro antes da LGPD, como no caso da legislação ambiental que, também em uma abordagem baseada no risco, exige a realização de Estudo de Impacto Ambiental (EIA) antes da realização de obra com potencial de lesar significativamente o meio-ambiente. Assim como uma construção é entendida como um processo capaz de, de forma não intencional, lesar o meio-ambiente, a LGPD parte do princípio de que externalidades que compõem os processos de tratamento de dados também comportam o risco de efeitos negativos e violação de direitos (BELLI, 2021).

É com isto em mente que o legislador determina a elaboração de RIPD sempre que o tratamento venha a pôr em risco liberdades civis e direitos fundamentais. Diante do exposto, resta evidente que a maioria das operações de tratamento de dados realizadas em cidades inteligentes representam risco às liberdades e aos direitos, haja vista a extensa incidência dos sensores, o aumento de poder do Estado e das empresas, o risco de violação da privacidade, os graves danos causados por incidentes de segurança da informação, entre outros fatores.

No Brasil, ainda dependemos da ANPD para fornecer maior detalhamento sobre quando deve ser ou não realizado um RIPD ou sobre o que deve conter no documento. Em maio de 2021, o órgão divulgou processo de tomada de subsídios sobre o RIPD, buscando colher opiniões por parte do setor privado e dos especialistas. Dentre as perguntas, a ANPD questionou quais elementos devem conter no RIPD, como esse deve ser avaliado pelo órgão, quando o documento deve ser elaborado, dentre outras perguntas (ANPD, 2021). Para o contexto das cidades inteligentes, as seguintes se destacam:

> A publicação de um RIPD pelo poder público deve ser feita em sua íntegra? (Art. 32 da LGPD) Por quê? Caso negativo, quais são os elementos que devem ser publicados e quais devem ser retirados da versão pública? (...) De que maneira o segredo comercial ou industrial poderá limitar o conteúdo de um RIPD? (ANPD, 2021).

A resposta a essas perguntas será essencial para entendermos o papel que a transparência irá cumprir nas cidades inteligentes, já que o RIPD fornece mecanismos essenciais para que a sociedade conheça as características e os riscos das atividades de tratamento. A delimitação do que constitui ou não segredo comercial ou industrial é importante, também, para que estes conceitos não se transformem em barreira intransponível para a transparência. Isso é especialmente relevante nas cidades inteligentes, nas quais os sistemas são utilizados para prestar serviços à população, que tem direito de conhecer o seu funcionamento.

Enquanto a Autoridade não conclui as suas considerações, podemos seguir com o exemplo da legislação europeia, que define três situações em que a elaboração de um RIPD será obrigatória: avaliação sistemática e completa de aspectos pessoais de pessoas singulares (como o perfilamento), tratamento em larga escala e controle sistemático de áreas públicas (BELLI, 2021). O legislador europeu determinou que tais práticas - amplamente adotadas em *smart cities* – merecem maior atenção, sendo o RIPD o mecanismo ideal para avaliação dos riscos existentes e adoção de medidas mitigadoras.

Quanto ao processo de elaboração, entende-se que este deve ser inserido dentro do programa de governança de dados de um controlador, sendo parte integral de seu programa de cumprimento à lei, devendo sempre ser realizado antes da implantação da operação avaliada (VAINZOF, 2019). O RIPD guarda proximidade com o conceito de *Privacy by Design*, que busca garantir a privacidade desde antes do início do tratamento de dados, o que tem relevância durante o planejamento de serviços inteligentes urbanos, que devem ser desenhados tendo os riscos à privacidade em mente (SETO, 2015). No que diz respeito ao seu conteúdo, a LGPD também 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 (VAINZOF, 2019).

Na Bélgica, o projeto SPECTRE (*Smart city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem*)[33] realizou diversos estudos avaliando a aplicação dos RIPD em projetos de cidade inteligente, atingindo conclusões que podem ser de grande valor para agentes envolvidos na

[33] Trata-se de iniciativa da Fundação de Pesquisa de Flandres (FWO), em parceria com a Universidade KU Leuven e a Vrije Universiteit Brussel.

implantação destes. Dentre as principais conclusões do projeto, entende-se que a elaboração do RIPD é essencial para que, nas cidades, 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). Entretanto, nem sempre este processo será simples ou de baixo custo, o que determina que o gestor busque a forma mais eficiente de conseguir realizá-lo. Segundo o projecto SPECTRE, o custo de elaboração de um RIPD aumenta na medida em que uma cidade inteligente se torna mais complexa. Diante do elevado custo de realização de um RIPD, a pesquisa conclui, mediante entrevistas, que encarregados (DPO) do setor público se mostraram mais propensos a implementar as avaliações de impacto em suas rotinas (VANDERCRUYSSE; BUTS; DOOMS, 2019).

Ainda que o custo de elaboração de um RIPD possa ser elevado, cabe à Administração Pública determinar que a sua elaboração prévia é obrigatória no contexto das cidades inteligentes. Cabe ao Estado assumir a obrigação de realizar e promover a realização de RIPDs pelos agentes privados que operarem serviços em cidades inteligentes. A existência de um mecanismo recorrente de mapeamento e mitigação dos riscos é forma eficiente de redução da verticalidade característica das cidades inteligentes, impostas como uma solução única e pouco transparente. 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.

Ressalte-se, aliás, que a elaboração do documento pode ser realizada para serviços complexos, que compreendem mais de uma atividade de tratamento de

dados, como se vê pela criação de modelos públicos de RIPD para serviços de redes inteligentes de energia (*smart grids*). Os dados que transitam nessas redes permitem a identificação precisa de comportamento de famílias, já existindo diversos modelos de RIPD para sua implantação (SETO, 2015). Também já foram implantados RIPD para serviços de cartões inteligentes, outro tipo de serviço amplamente utilizado nas *smart cities* (EDWARDS, 2016).

Apesar de a obrigatoriedade da realização de RIPD nas cidades inteligentes ser clara, ainda existem dúvidas relevantes sobre quem deve ser o protagonista na elaboração (o Estado ou o parceiro privado), sobre quando este deve ser elaborado e sobre o que deve constar exatamente no documento. Com relação a essas lacunas, cabe à ANPD a atuação proativa para definir diretrizes específicas para a elaboração de RIPD nas cidades, haja vista a redação do art. 32 da LGPD, que permite que a Autoridade defina quando e como agentes do Poder Público devem realizar avaliações de impacto.

Lilian Edwards (2016) ressalta que, apesar de isto ser difícil em cidades inteligentes que são construídas aos poucos, através de blocos inseridos em cidades já existentes, existe a possibilidade de elaboração de avaliações de impacto que abordem a cidade inteligente como um todo. Contudo, em projetos "*top down"* de construção de cidades inteligentes, como no caso de Songdo ou Masdar, é possível que já se pressuponha a elaboração de um RIPD como etapa prévia essencial. Trata-se de um processo capaz de mitigar a verticalidade e o déficit democrático de iniciativas deste gênero. Contudo, a autora alerta que a criação de RIPDs nesse contexto é uma meta ambiciosa, cuja efetividade ainda é objeto de dúvidas por parte da academia.

Vale mencionar que, além dos RIPD, as leis de proteção de dados costumam exigir a elaboração de outro relevante documento: o registro de operações de tratamento, comumente conhecido como RoPA (*record of processing activities*). Para a LGPD[34], a elaboração do registro de atividades de tratamento é uma obrigação de todo controlador e operador, apesar de a norma não prever detalhes sobre o que deve constar no documento. Ao contrário do RIPD, a principal função do mapeamento é a atribuição de base legal às operações de tratamento, buscando comprovar que todos os fluxos de uma organização cumprem com o princípio da

[34] "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (BRASIL, 2018).

finalidade. Conforme já exposto, a atribuição de base legal pode ser um desafio nas cidades inteligentes, o que põe a exigência da elaboração de RoPA em foco.

Não há, na pesquisa, uma exploração sistemática sobre a elaboração de RoPA no contexto de cidades inteligentes, sendo o documento compreendido como obrigação dos controladores e operadores que participarem das operações de tratamento de dados nas cidades. Contudo, é possível entender que a compilação de todos os projetos de *smart city* em um documento capaz de fornecer os principais fluxos de dados é um passo relevante para a garantia da governança de dados. No escopo de trabalho de um *city data officer* ou de um comitê de dados, é possível pensar que se inclua a obrigação de registro do tratamento de dados em projetos de cidade inteligente, a ser enviado pela ANPD ou acessado pela população através de mecanismos de acesso à informação pública, resguardado o segredo comercial e industrial.

Ao debater-se quais informações devem ou não constar em um mapeamento de dados, ainda estamos diante de uma lacuna legal, já que não há tal definição na LGPD e o tema ainda pende de regulação pela ANPD. Contudo, a partir do estudo da experiência europeia e das principais práticas de mercado, é possível entender que devem constar, pelo menos, as seguintes informações: descrição do tratamento de dados (fluxo, finalidade, tipos de dados, categorias de titulares afetados, terceiros envolvidos), atribuição de base legal, medidas de segurança e prazos de retenção e eliminação da informação (BRUNO, 2019).

A criação de documentos regulatórios previstos pela LGPD, como o RIPD e o registro de operações, com foco especial em cidades inteligentes é um passo que pode levar estes projetos por um caminho de maior segurança, planejamento e transparência, além de fornecer mecanismos de *accountability* para os atores envolvidos. Ainda, devemos lembrar que a CBCI define que a governança de dados é um dos objetivos estratégicos (Objetivo Estratégico nº 3) para a criação de cidades inteligentes brasileiras, sendo a elaboração de documentos de registro e avaliação de impacto uma etapa da garantia de promoção do cumprimento da LGPD (3.2) e de maior transparência nas operações de tratamento (3.3).

Por fim, deve-se ressaltar que não é possível, no contexto das cidades inteligentes, que um agente de tratamento obtenha a dispensa de elaboração de RIPD ou RoPA sob justificativa de ser agente de pequeno porte. Isto pois a Resolução CD/ANPD Nº 2/2022 estabelece, em linhas similares ao GDPR, que é

considerado de alto risco o tratamento de dados em larga escala ou capaz de violação de direitos e liberdades. Ambas as características estão presentes no tratamento de dados em cidades inteligentes, o que impossibilita a dispensa de obrigações da LGPD com base na configuração de agente de pequeno porte.

4.2. *Privacy by Design* e *Privacy Enhancing Technologie*s (PETs)

Conforme exposto, grande parte dos problemas relacionados à proteção de dados nas cidades inteligentes diz respeito ao fato de que, no planejamento destas, a privacidade não é um indicador avaliado com a merecida relevância. A maioria dos *rankings* de cidades inteligentes valoriza a sustentabilidade, a eficiência em serviços públicos e outros indicadores, praticamente sem mencionar a capacidade que a *smart city* tem de operar sem violar direitos como a proteção de dados.

Fato é que esta não é uma visão inédita que surge com as cidades inteligentes. Com o avanço da computação, a proteção de dados já foi vista como um entrave para o desenvolvimento tecnológico e econômico, sendo considerada um encargo para empresas, engenheiros e desenvolvedores (EDWARDS, 2016). Tendo isso em vista, emerge a noção de que a privacidade deve ser inserida na arquitetura dos projetos, o que é explorado no conceito de *privacy by design* (PbD) inaugurado por Ann Cavoukian.

Trata-se de uma visão que busca inverter a lógica: se a tecnologia era vista como uma ofensora costumeira, ela passa a ser utilizada para garantir a proteção da privacidade, o que guarda relação íntima com as *Privacy Enhancing Tecnologies* (PETs), que podem ser traduzidas como tecnologias potencializadoras da privacidade. O PbD se orienta por sete princípios: (i) a atuação proativa e preventiva; (ii) privacidade como padrão; (iii) privacidade inserida na arquitetura do sistema e nas práticas de negócio; (iv) funcionalidade completa; (v) segurança em todas as etapas; (vi) transparência e (vii) respeito pela privacidade do titular (LEMOS; BRANCO, 2021).

Desenvolvendo estes princípios para uma aplicação prática, podemos identificar algumas ações que os viabilizam, como a minimização de dados coletados, a segregação de bases de dados, a garantia da transparência ao usuário, o fornecimento de mecanismos de controle ao titular, entre outros. Além de serem boas práticas para a proteção de dados pessoais, os princípios do PbD se manifestam

na principiologia e nas normas da LGPD, que determina (art. 46), que os agentes de tratamento devem garantir a segurança em todo o ciclo de vida dos dados (LEMOS; BRANCO, 2021).

Estes valores e condutas devem ser inseridos em todo projeto de cidade inteligente, buscando mitigar os riscos que estes comportam. Neste sentido, pode ser oportuna uma alteração do Estatuto das Cidades (Lei Federal nº 10.257 de 2001) que, em suas diretrizes gerais, não possui norma específica para a aplicação responsável e segura das TICs. Ressalte-se que a norma foi elaborada em outro contexto em que nem sequer se imaginava a construção de cidades inteligentes como hoje. Entretanto, a sua atualização faz-se urgente, já que a norma se está defasada diante da forma contemporânea de criar e modificar cidades.

Uma das formas mais evidentes de inserção do PbD nas cidades é a já mencionada elaboração dos RIPD, que devem ser elaborados previamente para avaliar a necessidade, proporcionalidade e licitude de projetos envolvendo operações arrojadas de tratamento de dados pessoais (EDWARDS, 2016). Ainda, a LGPD estabelece que agentes de tratamento poderão estabelecer boas práticas setoriais (art. 50) para o processamento de dados. Isto deve ser estimulado pela ANPD, em cuja competência também se inclui a elaboração de normas de boas práticas a serem cumpridas pelo Poder Público. Em tais disposições, os princípios de PbD devem orientar as boas práticas em cidades inteligentes, fornecendo um rol de condutas que deve ser observado por todos os atores.

Indo além das medidas administrativas e organizacionais, o PbD também possui uma faceta técnica, que se conecta às mencionadas PETs ou tecnologias potencializadoras da privacidade. Essas técnicas se inserem sob um denominador comum de serem tecnologias que atuem para facilitar a privacidade, fazendo parte da metodologia do PbD (BIONI, 2021). O presente trabalho não busca e nem é capaz de realizar uma análise aprofundada das diversas PETs aplicáveis às cidades inteligentes, apesar de já existirem trabalhos que objetivam o arrolamento e detalhamento destas[35]. Entretanto, é possível explicar de que forma estas devem se relacionar com a construção de cidades inteligentes.

[35] Para maior detalhamento sobre os tipos e o funcionamento das PETs aplicáveis às cidades inteligentes, Curzon, Almehmadi e El-Khatib (2018) exploraram diversas modalidades aplicáveis às tecnologias utilizadas nas cidades, como a IoT, o tratamento em nuvem, entre outras. Por sua vez, Eckhoff e Wagner (2018) estabelecem um rol de PETs que pode ser aplicado de acordo com o serviço prestado na cidade. Já Martinez-Ballesté et al. (2013) realizam uma contraposição entre as

Cabe mencionar a separação da privacidade em dimensões exposta acima (item 3.1, tabela 2), que possibilita determinar quais tecnologias devem ser usadas para a proteção de cada dimensão da privacidade. Existem, por exemplo, aquelas mais capazes de garantir a proteção da identidade (como a anonimização ou técnicas de privacidade em videovigilância) e outras que devem ser aplicadas para garantir o sigilo da localização do usuário (como o mascaramento de localização). Para ilustrar a aplicação de uma PET, é possível imaginar que um serviço que dependa da localização do titular (LBS), como o fornecimento de recomendações de serviços de saúde próximos, adote tecnologia que mascare a localização durante o tráfego da informação (MARTINEZ-BALLESTÉ et al., 2013).

Ainda, é importante entender que a aplicação de PETs nas cidades inteligentes atua em duas categorias: técnicas de anonimização e de garantia da segurança. A grande maioria dessas atuará de forma a anonimizar, encriptar ou embaralhar bases de dados para impedir usos ilícitos da informação ali armazenada, impedindo ou dificultando a ocorrência de incidentes. Para uma aplicação bem-sucedida, o administrador também deve ser capaz de entender as camadas em que deve atuar, podendo utilizar PETs que se aplicam aos sensores, às redes e às aplicações (CURZON; ALMEHMADI; EL-KHATIB, 2018).

Diante da dependência que as *smart cities* possuem de dispositivos de internet das coisas (IoT), o administrador deve estar atento para as PETs especificamente pensadas para esses dispositivos. Sendo a IoT um dos principais desafios para a garantia da proteção de dados, diversos tipos de PETs são explorados como forma de promover a segurança e a interoperabilidade entre dispositivos (BIONI, 2021). Uma abordagem promissora para a criação de PETs dedicadas à internet das coisas deriva dos estudos baseados na tecnologia *blockchain*, que será abordada no item 4.5.

Por fim, devemos entender que a aplicação de PETs, por mais urgente que seja, ainda representa um desafio tecnológico, sendo difícil inserir a privacidade no código de diversas aplicações. Nesse sentido, Edwards (2016) alerta que a tecnologia não pode ser vista como uma solução infalível, devendo ser combinada com soluções de ordem administrativa e cultural, sendo a organização do Estado e a conscientização da população tão importante quanto as PETs. Em suma, a autora

---

dimensões da privacidade (localização, identidade, pegadas digitais, propriedade e consultas) e as PETs aplicáveis a estas.

entende que o principal caminho para a instituição bem-sucedida do PbD nas cidades inteligentes é inserir o cidadão no foco dos projetos, como sujeito de direito e protagonista. Para isso, precisamos entender o que o cidadão espera da cidade inteligente e como aproximá-lo dos projetos de *smart city*.

4.3. Entender as preocupações e 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, já mencionado, 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 cuja adesão é essencial para o sucesso da *smart city*. Assim, é essencial entender o que este cidadão pensa sobre a cidade e os riscos nela existentes, verificando se este se sente seguro para interagir com o ambiente urbano interconectado. 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 para o cidadão. É o que explicam Finch e Tene (2016, p. 1608):

> Visões populares de cidades futuristas (cada vez mais tendendo para a distopia) geralmente ilustram tecnologias de vigilância inconfiáveis e ubíquas, mostrando sensores urbanos e câmeras que operam como ferramentas da repressão e estagnação em vez de transparência e inovação. Tecnologias de cidade inteligente, nessa ótica, são controversas e opacas, enquanto, na verdade, não precisam o ser. O objetivo de governos locais, desenvolvedores de internet das coisas e urbanistas deve ser empoderar e engajar os cidadãos, para 'levá-los consigo' na jornada pela tecnologia[36].

[36] "Popular visions of futuristic cities (increasingly trending towards the dystopic), often illustrate untrustworthy, ubiquitous surveillance technologies, setting urban sensors and cameras operating as tools of repression and stagnation rather than transparency and innovation. Smart city technologies, in this optic, are adversarial and secretive; in reality, they need not be. The goal of local governments, Internet of Things developers and urbanists should be to empower and engage citizens—to "bring them along for the technology ride.". Tradução livre

Para melhor avaliar como proporcionar uma boa experiência para o cidadão, Lisbet Van Zoonen (2016), pesquisadora da Universidade Erasmo de Roterdã, elaborou uma metodologia que, em confronto com pesquisa empírica, é capaz de mapear as preocupações deste na cidade inteligente. Para isso, a autora realiza uma comparação entre duas variáveis, que são o tipo de dado (pessoal ou impessoal) e a finalidade do tratamento (prestação de serviço ou vigilância), de modo a entender a melhor maneira de estabelecer cada projeto de *smart city*.

Em primeiro, é preciso entender que nem toda aplicação de cidade inteligente dependerá do uso de dados pessoais, ou seja, de informação capaz de identificar uma pessoa natural. Muitos projetos são baseados somente em dados que não remetem a pessoas, como os índices locais de poluição ou consumo de energia. Naturalmente, as preocupações no que diz respeito à informação impessoal é menor do que quanto ao tratamento de dados pessoais[37]. Em seguida, deve ser avaliada a finalidade do tratamento que se divide, em geral, na prestação de serviços públicos ou na expansão da vigilância. Neste ponto, os cidadãos demonstraram maior boa vontade em ceder seus dados diante de um retorno na forma de serviços públicos e maior receio quanto aos fins de vigilância.

Realizando essa comparação entre tipo de dado e finalidade, a autora resume sua metodologia no seguinte quadrante (figura 1). Assim, existem quatro cenários possíveis: o tratamento de dados pessoais para prestação de serviços (quadrante I), o tratamento de dados pessoais para vigilância (quadrante II), o tratamento de dados impessoais para vigilância (quadrante III) e o tratamento de dados impessoais para prestação de serviços (quadrante IV).

[37] Neste ponto, a autora faz dois destaques relevantes: em primeiro, a concepção popular sobre o que é ou não informação pessoal é imprecisa, já que muitos cidadãos consideram dado pessoal somente a informação íntima ou sensível. Em segundo, alerta que é necessário termos cuidado ao atribuir a característica de "impessoal" a grupos de dados, diante das amplas técnicas de reidentificação de dados anonimizados existentes (VAN ZOONEN, 2016).

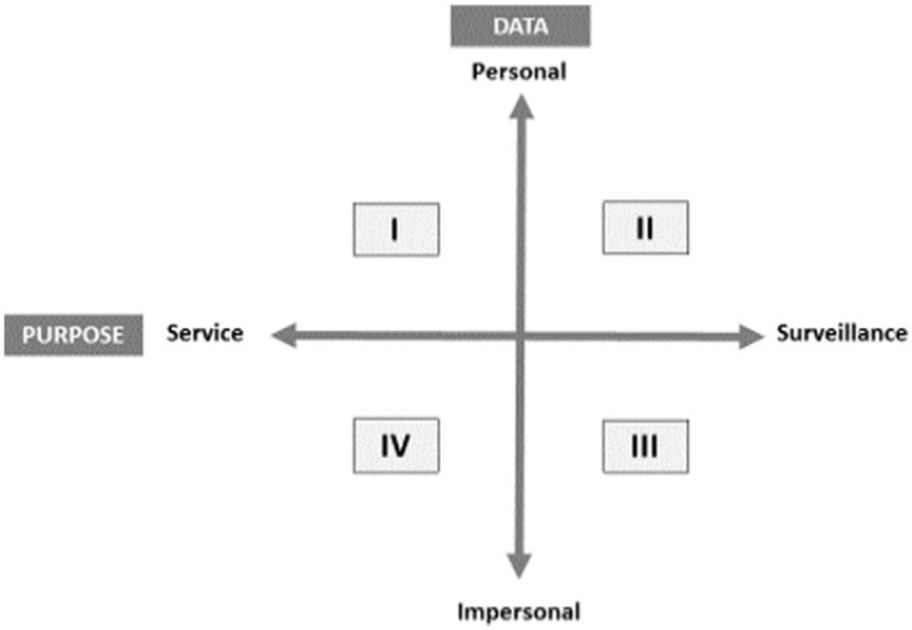

Figura 1 - Método de medição da expectativa de titulares. Fonte: VAN ZOONEN, 2016

No primeiro cenário (uso de dados pessoais para prestação de serviços), os desafios são moderados, devendo o administrador avaliar de que forma cumprir a lei ao prestar os serviços ao cidadão. Tal atividade deve ser feita com cuidado para evitar a coleta excessiva de dados, o que pode fazer o cidadão suspeitar do uso de suas informações para fins de vigilância. Isso faria o projeto se mover para o segundo quadrante, onde se concentra a maioria das preocupações dos cidadãos, que receiam o uso de dados para a expansão do aparato de controle estatal.

Em seguida, o uso de informações não identificadas para o policiamento também deve ser objeto de atenção, já que mesmo esse tipo de informação pode vir a ser conectada a uma pessoa (através, por exemplo, de reconhecimento facial). Além disso, mesmo informações estatísticas podem ter efeito social nocivo, como o eventual registro de aumento da repressão policial em áreas consideradas "estatisticamente perigosas". Por fim, o quadrante de menor risco é o uso de dados não identificados para prestação de serviços, devendo o administrador ter cuidado somente com a possibilidade de reidentificação dos dados (VAN ZOONEN, 2016).

A partir dessa metodologia, é possível que o gestor público tenha a capacidade de mapear a melhor forma de estabelecer projetos de cidade inteligente. Vejamos os seguintes exemplos.

Uma das tecnologias mais comuns em *smart cities* são as lixeiras inteligentes, que são capazes de monitorar a quantidade de lixo para avisar à

administração quando necessitam ser esvaziadas, o que reduz os custos com logística. Essa técnica pode ser aplicada de formas com impacto distinto na privacidade. Van Zoonen (2016) explica que, como forma de prevenir que lixeiras inteligentes de bairros sejam usadas para atividades ilegais, algumas cidades criaram cartões inteligentes para permitir que somente os habitantes locais as utilizem. Apesar da boa intenção, tal projeto gera preocupações muito maiores de violação à proteção de dados, já que o serviço público passa a demandar a inserção de dados pessoais, o que certamente não é necessário em uma política de gestão inteligente de resíduos.

Outro exemplo é o caso do monitoramento de redes sociais, prática comum em cidades, que pode ser realizada com finalidades diversas. A prefeitura de Roterdã possui mais de 30 contas em redes sociais para interagir com os cidadãos e fornecer informações sobre a cidade. Neste processo, a administração colhe dados de natureza essencialmente pessoal, com a intenção de prestar um serviço e dar maior retorno ao cidadão sobre as atividades do Estado. Entretanto, sobram caso autoridades de segurança monitorem redes sociais com fins de fiscalização de comportamentos e vigilância, isto certamente gerará maior desconfiança por parte dos cidadãos em sua interação com a *smart city*.

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 (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 ou insegura, potencializando a *accountability* na cidade inteligente (FINCH; TENE, 2016).

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 estabelecer maneiras de 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 e a participação cidadã. Tanto o direito de acesso quanto a criação de portais de dados abertos são iniciativas ligadas à promoção da transparência, que será abordada na seção seguinte.

Por fim, cabe mencionar que a sensação social quanto à privacidade pode ser um indicador perigoso em determinados contextos, já que nem todos os setores da sociedade são capazes de mensurar o que está em jogo na economia movida a dados. Locais com acesso dificultado à educação ou comunidades compostas por grupos majoritariamente idosos podem ter dificuldade na interação com a cidade inteligente. Ademais, comunidades vulneráveis possuem preocupações com assuntos mais graves e urgentes que a proteção de dados pessoais, muitas vezes ainda esperando a realização de direitos humanos básicos (BREUER; VAN BRAKEL, s. d.). Estes grupos mencionados podem acabar aceitando ceder seus dados em iniciativas de pouco retorno positivo.

Willems et al. (2017), por exemplo, realizaram pesquisa empírica com base na seguinte pergunta: "a privacidade afeta a participação cidadã nas *smart cities*?". Apesar de limitações metodológicas, os autores afirmam que, ainda que cidadãos demonstrem preocupação com a privacidade, estes geralmente optarão por participar da cidade inteligente de qualquer maneira. Ainda, os autores concluíram que as pessoas, em geral, estão dispostas a trocar dados pessoais por maior eficiência nos serviços urbanos.

Em conclusão, ainda que o administrador tenha o dever de mapear as expectativas dos cidadãos quanto aos projetos na cidade inteligente, este é obrigado a respeitar a privacidade ainda que os habitantes estejam dispostos a ceder seus dados de forma acrítica. Não é porque parte da população não questiona ou não entende como ocorre a violação ao direito à proteção de dados que o administrador é autorizado a agir de forma inconsequente. Neste ponto, é importante que as autoridades de proteção de dados, como a ANPD, fiscalizem os processos de tratamento de dados em *smart cities*. Ademais, é responsabilidade do Poder Público

promover a conscientização sobre os riscos e potencialidades do tratamento massivo de dados nas cidades[38].

4.4. Efetivando a transparência nas cidades inteligentes

Um dos caminhos para a promoção da confiança acima mencionada é garantir que as cidades inteligentes sejam transparentes em seu funcionamento. A transparência é um dos princípios elencados pela LGPD, atuando no sentido de que os agentes de tratamento de dados devem fornecer, aos titulares, informações claras sobre as suas operações. Tal princípio tem fundamento no fato de que titulares e agentes se encontram em desequilíbrio de poder, tendo o titular pouca ou nenhuma capacidade de saber por si só como cada controlador atua.

Apesar de aparentemente antagônicos, privacidade e transparência podem operar em uma sinergia que promove a legitimidade das cidades inteligentes. Privacidade e proteção de dados são conceitos que vão além da mera garantia de sigilo, incluindo também o empoderamento do titular de dados com mecanismos que lhe permitem saber como e para que seus dados são coletados e tratados (DONEDA, 2019). Logo, não há controvérsia entre as garantias, desde que iniciativas de transparência sejam pensadas para que não haja exposição de dados desnecessários para a finalidade desejada.

Nas cidades inteligentes, tais iniciativas de transparência podem ser de governo aberto, promover a transparência algorítmica ou então fornecer informações sobre as atividades de tratamento realizadas sobre os dados dos cidadãos. Em primeiro, as iniciativas de governo aberto se fundamentam na defesa do *open data* (dados abertos), que serve para abrir os repositórios de dados públicos à sociedade, o que deve ser contraposto à proteção de dados pessoais. No que diz respeito à transparência algorítmica, esta se opõe à opacidade das tecnologias de tratamento de dados, pouco claras para os cidadãos. Por fim, a transparência organizacional busca demonstrar, à população, as características das operações de processamento empreendidas na cidade inteligente.

[38] Neste ponto, é importante ter em mente que grande parte dos alvos dessas campanhas de conscientização pode ter dificuldade de entender as informações divulgadas, seja por deficiência na alfabetização ou pela pouca familiaridade com a tecnologia. O gestor deve promover a linguagem simples e direta e evitar o linguajar técnico e demasiadamente jurídico comom às políticas e avisos de privacidade tradicionais (BREUER; VAN BRAKEL, s. d.).

4.4.1. Iniciativas de dados abertos (*open data*) e transparência algorítmica

Ainda que se fuja do clichê que compara o valor dos dados ao do petróleo, é inegável que o acesso a dados se tornou economicamente atrativo, além de fornecer oportunidades para que a sociedade conheça e enfrente seus problemas. Até a revolução tecnológica das últimas décadas, os maiores coletores de dados da história sempre foram os governos, sendo estes dotados de registros diversos, funcionários especializados e competência legal para coleta, organização e processamento de informações sobre as pessoas e lugares.

Historicamente, essas informações eram guardadas em arquivos fechados e, nas ocasiões em que se obtinha acesso, os dados eram de difícil interpretação e organização (KITCHIN, 2014). Em reação a isso, leis de acesso à informação pública são editadas desde o século XVIII, quando a Suécia editou a primeira lei que garantia o direito à informação. Hoje, já são mais de 100 países que garantem aos cidadãos o direito de exigir informação pública (DAVIES, 2020). No Brasil, trata-se da Lei de Acesso à Informação (Lei Federal nº 12.527 de 2011), que obriga o Estado a adotar, no tratamento de dados públicos, a publicidade como regra e o sigilo como exceção. Ainda, o já mencionado princípio do livre acesso previsto pela LGPD, busca dar aos titulares informações sobre o tratamento de seus dados de forma gratuita e facilitada.

Contudo, com o avanço da computação e do processamento de dados, passou-se a entender que a mera divulgação de documentos em estado bruto não seria suficiente para garantir o direito de acesso. Hoje, entende-se que os governos devem garantir acesso a bases de dados, tendo o cidadão o direito de acessar e utilizar esses dados de forma aberta. É essa a base do movimento por dados abertos (*open data*), que entende que a efetivação do direito de acesso deve incluir a publicação de dados em formato legível por máquina, de acesso livre e licença aberta (KITCHIN, 2014).

Este movimento, que se baseia na cultura *hacker*, entende que os cidadãos tem o direito de utilizar essas informações para seus propósitos, fazendo com que a coleta de dados pelo Estado forneça oportunidades à sociedade civil e ao setor privado. O acesso a informações públicas permite, por exemplo que a sociedade se organize em torno de bens comuns para desenvolver iniciativas de participação na construção da cidade (MOROZOV; BRIA, 2019). Já para a atividade econômica, a

abertura de dados permite que empresas coletem e reutilizem essas informações para desenvolvimento e criação de produtos.

Além de trazerem oportunidades de utilização dos dados públicos, iniciativas de dados abertos também promovem a responsabilização (*accountability*) dos gestores públicos e a participação cívica na democracia (KITCHIN, 2014). O escrutínio permite que a sociedade seja capaz de interpretar como a cidade inteligente está utilizando o dinheiro arrecadado e quais decisões políticas sua administração está tomando. Ainda, conforme mencionado, a abertura de dados e a possibilidade de sua reutilização geram confiança na população, podendo aproximar Estado e sociedade em seus objetivos comuns.

Essas iniciativas de dados abertos, por sua vez, ressoam em projetos de cidade inteligente, que geram uma quantidade impressionante de dados que podem ser publicados de diferentes maneiras. Apesar de muitas cidades inteligentes se dizerem *open data*, essas iniciativas possuem diferentes graus de participação popular, podendo servir como forma de simular o ativismo cívico ou para efetivamente conceder aos cidadãos o controle sobre os dados gerados pelo Estado (DAVIES, 2020).

Ou seja, além da mera garantia de publicação de dados, especialistas entendem que existe a necessidade de que haja uma infraestrutura de dados públicos que seja capaz de trazer benefícios à sociedade. Ao falarmos de infraestrutura urbana, pensamos em pontes, prédios e ruas, mas cidades inteligentes dependem de uma chamada infraestrutura de dados, que inclui artefatos físicos e digitais. Estamos falando de bases de dados, *dashboards*, sistemas de intercâmbio de dados (*application programming interfaces* – APIs), algoritmos, entre muitos outros exemplos (DAVIES, 2020).

Para que os dados da cidade sejam de fato abertos e reutilizáveis, essa infraestrutura deve ser de fácil acesso e integrada, evitando que se criem silos de dados que não se relacionam. Também é necessário evitar a prática de *data dumping* (despejo de dados), que consiste na mera publicação de grandes bases de dados em formato bruto. Para que as cidades consigam realizar o potencial do movimento *open data*, os cidadãos devem ser capazes de participar não só do acesso às bases de dados, mas também da produção dos dados e do desenho dessa infraestrutura de dados (DAVIES, 2020). É somente conhecendo tal infraestrutura que a sociedade pode decidir a melhor forma de usá-la, o que demanda que as cidades estejam

dispostas a ir além da mera publicação de dados, convidando a sociedade a participar do debate sobre a infraestrutura tecnológica.

Entretanto, iniciativas de dados abertos não devem ser vistas como uma panaceia, já que incluem uma variedade de arquiteturas possíveis, todas elas trazendo desafios significativos. Cabe ressaltar que a criação e manutenção de robustas estruturas de dados abertos é uma missão cara, podendo ser inviável para grande parte das cidades que buscam se tornar inteligentes (KITCHIN, 2014). Ainda, em um contexto cada vez maior de participação de empresas privadas na prestação de serviços de *smart city*, existe uma preocupação sobre a privatização de informações de natureza pública, o que pode reduzir as oportunidades de acesso e uso destas (DAVIES, 2020).

Apesar da centralização de bases de dados públicos ser positiva para questões de acessibilidade e interoperabilidade, tal característica também é motivo de alguma preocupação. Isto pois a publicação deve ser feita de forma cuidadosa para que não se viole o princípio da necessidade, que demanda o tratamento da mínima quantidade de dados necessária para o atingimento da finalidade. Ou seja, bases de dados públicas devem ser construídas com o cuidado de não violar a intimidade de indivíduos. Por outro lado, devemos ter atenção para a mobilização deste argumento como forma de permitir a não divulgação de dados de natureza pública pelo Estado[39], o que exige um difícil equilíbrio entre acesso à informação e proteção de dados pessoais.

Indo além dos dados abertos, a efetivação da transparência na cidade inteligente depende do conhecimento, pelos cidadãos, dos critérios utilizados para analisar a sua informação. O tratamento de dados é feito através de algoritmos protegidos por sigilo comercial e industrial e de funcionamento pouco transparente para a sociedade. Sem entender de que forma sua informação é processada pela cidade inteligente, o cidadão não tem como saber como é visto pelos sistemas utilizados pela cidade, o que baseia os pedidos pela chamada transparência algorítmica.

[39] Especialistas em acesso à informação pública denunciam que o Governo Federal utiliza a Lei Geral de Proteção de Dados como argumento para não divulgar bases de dados de divulgação obrigatória, mobilizando a privacidade como forma de se escusar do cumprimento de obrigações legais (IGNACIO, 2022).

A demanda por transparência no funcionamento de algoritmos é uma das principais causas no debate sobre regulação da tecnologia, já 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, analisando anteriormente (MULHOLLAND; FRAJHOF, 2020).

Logo, o tratamento de *big data* urbano, apesar das inúmeras potencialidades geradas, também gera externalidades negativas. Mesmo o uso de dados precisos pode gerar consequências discriminatórias ou imprecisas, o que demanda que a transparência no tratamento de dados vá além da informação sobre quais tipos ou qual volume de dados são tratados. Deve ser garantido, aos cidadãos, uma espécie de transparência potencializada, que permita o acesso ao critério utilizado para a tomada de decisões. Ou seja, além da prevenção à criação de bases de dados secretas, a transparência algorítmica objetiva a prevenção a usos ilícitos e pouco claros de dados pessoais (FINCH; TENE, 2016).

A exigência de maior clareza sobre o funcionamento de algoritmos utilizados em cidades inteligentes deve ser equilibrada com a existência de segredo industrial e comercial. Tais informações proprietárias não devem ser divulgadas, sob pena de constrição da inovação e da livre iniciativa. Contudo, é exigível que se explique o funcionamento de um sistema da forma mais eficiente e detalhada possível, de modo a termos maior transparência algorítmica.

Além da já analisada revisão de decisões automatizadas, uma das principais formas de se promover a transparência algorítmica é a criação 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 e Bria (2019) consideram que o setor público deve dar à sociedade a capacidade de direcionar a inovação e reverter a lógica verticalizada de construção de cidades inteligentes. Por isso, afirmam:

> O setor público tem um papel estratégico a desempenhar na indicação da direção a ser dada para a mudança, que poderá ser objeto de soluções desenvolvidas de baixo para cima. A prioridade deve ser então a orquestração de ecossistemas de inovação como um todo por meio de políticas públicas fortes (...) (MOROZOV; BRIA, 2019, p. 149)

Exemplos de uso de códigos abertos e *softwares* livres podem ser verificados em diversos projetos de cidade inteligente pelo mundo, como Barcelona. A cidade catalã utiliza a plataforma Sentilo, que se descreve como uma plataforma cooperativa de cidades inteligentes, utilizando código livremente acessível para que a cidade seja menos dependente de plataformas proprietárias e de funcionamento obscuro[40]. O uso de sistemas transparentes e de soluções colaborativas permitem, ao mesmo tempo, que a sociedade tenha ciência de como suas informações são tratadas e que possa colaborar com o debate sobre o direcionamento da inovação urbana.

A transparência algorítmica é, aliás, parte integrante dos projetos de dados abertos, já que a mencionada infraestrutura informacional da cidade pode ser construída de formas mais livres ou mais dependentes de soluções proprietárias ou pouco transparentes. Grande parte da infraestrutura digital advém de poucos fornecedores, o que gera o risco de que as redes digitais e bases de dados se vejam presas em jardins murados (*walled gardens*) baseados em tecnologia proprietária (MOROZOV; BRIA, 2019).

Morozov e Bria (2019) relembram que essa característica vai contra os princípios iniciais da internet, originalmente distribuída, horizontal e aberta. Contudo, hoje, a maioria das *smart cities* utiliza sistemas operacionais urbanos proprietários, o que favorece a expansão de projetos pautados na coleta excessiva de dados pessoais e pouco influenciáveis pela população. Contra isso, a criação de ambientes de desenvolvimento tecnológico cooperativo oferece alguma resistência:

> A meta desse processo é a criar um ecossistema descentralizado de inovação que atraia uma massa crítica de agentes de inovação capaz de redirecionar a economia sob demanda centralizada e alimentada por dados em direção a uma economia descentralizada, sustentável e baseada em bens comuns. As iniciativas de dados da cidade abertos devolvem agência e controle aos cidadãos com o objetivo de instrumentalizar dados e informações coletivos para a melhora das condições de todos (MOROZOV; BRIA, 2019, p. 115)

[40] 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).

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 e conhecem os problemas que buscam solucionar. Dessa maneira, é possível reduzir a dependência de soluções universais, que nem sempre irão se amoldar às realidades locais. Isto é relevante em países periféricos, cujos problemas são de natureza distinta daqueles dos centros globais de produção de tecnologia (WILLIS; AURIGI, 2020).

Sennet considera que a criação de ambientes uniformes em lugares diferentes é a melhor forma de criar ambientes obsoletos, já que assim que "*as coisas passarem a ser feitas de maneiras diferentes, a forma fixa não servirá mais, ou então uma nova ferramenta virá a tornar obsoletas as velhas capacitações"* (2021, p. 187). Assim, a criação de soluções colaborativas e baseadas na realidade local permitem que a cidade inteligente seja mais resiliente e capaz de atender aos problemas concretos da região.

Para Willis (2020), a promoção de um urbanismo de código livre e aberto é a melhor aposta para que o papel dos dados nas cidades inteligentes seja pensado de forma responsável. Isto pois a criação colaborativa e pública de tecnologias urbanas permite que a sociedade discuta e escolha a melhor forma de utilização de dados pessoais para abordar problemas que ela própria conseguiu detectar e diagnosticar.

Sennet (2021) defende que a promoção do debate aberto e da inovação a partir de *feedbacks* da comunidade é uma forma de combatermos o urbanismo impositivo. Para isso, contribuem os projetos de código aberto, que encaram problemas urbanos sem ter "medo do acaso" (p. 186). Enquanto sistemas proprietários não recebem *feedback* por parte da comunidade, a cidade baseada em sistemas abertos é capaz de reconhecer as limitações em seus dados e de buscar relacioná-los com outros conjuntos. Trata-se, inclusive, de uma forma de legitimação democrática das cidades inteligentes, já que a adoção de soluções prontas carece do processo dialógico comum aos regimes democráticos.

Entretanto, não podemos subestimar as dificuldades que envolvem a criação destes projetos, que requerem grande dispêndio de recursos públicos e dependem

de uma comunidade capaz de compreender e participar do processo de desenvolvimento de tecnologia. Em um mundo marcado pela rápida urbanização na periferia do capitalismo, algumas cidades dificilmente terão como desenvolver a sua própria infraestrutura informacional. Logo, a realidade é que a implantação de serviços de *smart city* ainda dependerá de soluções proprietárias e já desenhadas anteriormente de forma universal, o que impõe um contínuo debate sobre transparência algorítmica e promoção dos direitos de proteção de dados.

4.4.2. Transparência organizacional

Além das medidas de dados abertos e transparência algorítmica, a promoção da transparência nas cidades depende da criação de documentos e plataformas que permitam a fácil interação do cidadão com a *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 sobre as operações de tratamento de dados.

A medida mais evidente para a promoção da transparência é a publicação de políticas ou declarações de privacidade, contendo os detalhes mais relevantes sobre as atividades de uma organização. A publicação desses documentos não é uma obrigação legal, mas deve ser avaliada positivamente pelo regulador, tendo em vista a necessidade de observação do princípio da transparência. Em regra, as políticas de privacidade costumam listar: os tipos de dados tratados, as finalidades de tratamento, as bases legais atribuídas, os limites do compartilhamento de dados com terceiros, os canais para atendimento aos direitos dos 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 (ECKHOFF; WAGNER, 2018). As empresas fornecedoras de tecnologia costumam ter políticas de privacidade para seus produtos, nas quais explicam o funcionamento destes. Porém, tendo em vista a proliferação de aplicações privadas utilizadas em serviços públicos urbanos, as cidades inteligentes devem ir além do mínimo praticado pelo mercado.

A publicação de políticas esparsas não é suficiente nas cidades inteligentes, haja vista que um dos principais desafios, para o cidadão, é entender quais dados

são coletados, por quem são tratados e para qual finalidade são utilizados. Além disso, o titular tem pouca visibilidade sobre o compartilhamento de suas informações na cidade inteligente. Por isso, políticas de privacidade em *smart cities* podem conter outros detalhes além dos citados, como avaliações de impacto realizadas sobre serviços ou detalhes sobre qual agente controla cada base de dado na cidade (FINCH; TENE, 2018).

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 é que estas cubram tanto a cidade como um todo quanto os serviços específicos nela prestados, tendo atenção à multiplicidade de formas de coleta e processamento de dados no ambiente urbano conectado (INTERNATIONAL STANDARDS ORGANIZATION, 2020).

Sendo assim, a promoção da transparência de uma cidade inteligente como um todo pode ser feita através de uma política de privacidade centralizada, que explique, em linhas gerais, os fluxos de dados dos principais serviços utilizados na 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. Ainda, em uma perspectiva de exercício de direitos dos titulares, a centralização de informações sobre a cidade em um único documento pode promover a responsabilização dos agentes de tratamento, fornecendo maior transparência e *accountability*.

Indo além do princípio da transparência, as políticas de privacidade para cidades inteligentes são essenciais para a demonstração do cumprimento dos princípios da finalidade e adequação. Isto pois devem listar quais dados são coletados e para qual objetivo, idealmente vinculando tais operações às bases legais previstas pela legislação local. Também é oportunidade para que o governo demonstre cumprir com a obrigação de limitar o tratamento à menor quantidade de dados necessários para o atingimento da finalidade. Neste ponto, pode ser relevante informar como e em que ocasião a administração fará uso de técnicas de anonimização e tratará dados anonimizados (FINCH; TENE, 2018).

Importante ressaltar, porém, 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 utilização

de linguagem puramente técnica, em um contexto de massa, é uma barreira à compreensão popular sobre o funcionamento de serviços que irão impactar a população em seu cotidiano. Cidades inteligentes também precisam ter atenção à população portadora de deficiências, o que impõe a publicação de documentos em formato que lhe atenda (FINCH; TENE, 2018).

Sendo assim, a criação de plataformas interativas, vídeos, cartilhas e outros recursos são iniciativas importantes para o sucesso da transparência organizacional em cidades inteligentes. Também é relevante, para a cidade, determinar onde esses documentos e plataformas serão localizados, devendo ser priorizada a facilidade de acesso. Como exemplo, é possível que o *link* ou código de acesso seja disponibilizado em áreas monitoradas por câmeras, o que servirá para promover os direitos dos cidadãos filmados. Ademais, atores urbanos devem ter em conta que uma estratégia de comunicação bem desenhada é essencial para o sucesso destes projetos, devendo elaborar campanhas que promovam a conscientização da população quanto à privacidade (FINCH; TENE, 2018).

Ressalte-se que, em comparação às medidas de dados abertos ou de transparência algorítmica, a promoção da transparência organizacional depende de investimento menos significativo, bastando a elaboração de documentos, webpages e plataformas. Ainda assim, são poucos os exemplos de aplicação dessas políticas de transparência organizacional, o que evidencia a já mencionada falta de cultura de proteção de dados nos projetos. Merecem destaque, porém, dois portais públicos: a página do governo indiano para cidades inteligentes (*Smart Cities India*) e as políticas da cidade estadunidense de Seattle.

A plataforma *Smart Cities India* (*smartcities.data.gov.in*) é o portal de dados abertos criado pelo Ministério de Habitação e Assuntos Urbanos da Índia, com intenção de promover a transparência e as diretrizes nacionais para cidades inteligentes. O site disponibiliza mais de 3,500 catálogos de dados públicos, além de listar os contatos dos encarregados de dados municipais. Ainda, a plataforma permite acesso imediato à estratégia indiana para cidades inteligentes e ao guia para avaliação de maturidade das cidades para temas de proteção de dados.

Já a cidade de Seattle, com a intenção de conciliar inovação e privacidade, inaugurou um robusto programa de adequação dos projetos de *smart city* aos melhores padrões de proteção de dados. Segundo seu portal oficial, o programa de privacidade foi criado com a intenção de encontrar o equilíbrio entre coletar dados

para prestar serviços e a necessidade de proteção da privacidade. Este programa foi iniciado em 2015, envolvendo 15 departamentos locais, políticos, membros da sociedade civil e pesquisadores (CITY OF SEATTLE, 2022a).

Neste processo, a cidade adotou seis princípios para o tratamento de dados no ambiente urbano. O documento, chamado de *City of Seattle Privacy Principles* (CITY OF SEATTLE, 2015), estabelece 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.

Como resultado do programa, a cidade já desenvolveu uma política de privacidade detalhada, que explica como se dá o tratamento de dados de: dispositivos móveis, serviços de saúde, serviços públicos, segurança, serviços financeiros, videovigilância e prestação de serviços online. Por fim, cabe ressaltar que a Prefeitura de Seattle já realizou mais de 100 avaliações de privacidade (RIPD), sendo 19 dessas disponibilizadas publicamente (CITY OF SEATTLE, 2022b). 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 o valor do *privacy by design*.

4.5. Possibilidades trazidas pela tecnologia blockchain

A aprofundada sobre a definição e o funcionamento da tecnologia *blockchain* é tarefa que excede o escopo desta pesquisa, sendo um desafio até para trabalhos que se dedicam ao assunto. Contudo, falar sobre inovação tecnológica e tratamento de dados e não mencionar a tecnologia *blockchain* parece ser cada vez mais difícil. Nas cidades inteligentes, não é diferente: são crescentes as aplicações e potencialidades nela baseadas. No que diz respeito à promoção de confiança do cidadão e de políticas de dados abertos, temas abordados nos itens acima, a tecnologia *blockchain* promete uma verdadeira revolução.

Antes de adentrar na explicação sobre o que é *blockchain*, entendemos que a tecnologia pode ser utilizada de duas formas principais nas cidades inteligentes: (i) como parte da arquitetura de soluções tecnológicas para a prestação de serviços

públicos e (ii) como uma forma de garantir a privacidade e segurança do processamento de dados nas cidades, atuando como tecnologia potencializadora da privacidade (PET). Em ambas as formas, considerações sobre o cumprimento das normas de proteção de dados se fazem necessárias. Contudo, antes disso, é preciso delimitar do que falamos quando falamos em *blockchain*.

A própria definição do que é *blockchain* é contenciosa e, muitas vezes, serve somente para a descrição de sistemas específicos, como a *blockchain* da criptomoeda *Bitcoin*. Em linhas gerais, entende-se por *blockchain* uma cadeia de dados capaz de registrar operações de maneira pública, cronológica, digital e imutável, atuando como uma espécie de livro-razão (*ledger*) digital. Cada bloco dessa cadeia constitui um registro criptografado conectado de forma linear a uma sequência de blocos (CHANG; ALMEIDA, 2020). Uma definição mais ampla adota a terminologia *distributed ledger technology* (DLT), que significa que a rede blockchain é capaz de registrar dados e transações de forma descentralizada e independente de um ponto central garantidor (RAMOS; SILVA, 2019).

Ao contrário das transações tradicionais, que dependem de um nódulo central (como os bancos) que verifica e autoriza cada transação, sistemas baseados em *blockchain* independem de uma autoridade central, já que cada etapa é verificada por todos os pontos da rede. Não à toa, a primeira aplicação da tecnologia foi a criação de uma moeda independente de qualquer autoridade garantidora, a *Bitcoin*. Mas, hoje estruturas em *blockchain* permitem aplicações muito mais amplas do que as criptomoedas, possibilitando o seu uso em diversos serviços de *smart city* (QI et al., 2017).

As principais características que tornam a *blockchain* interessante para as cidades inteligentes são: (i) transparência, já que todas as transações são registradas e visíveis para toda a rede; (ii) descentralização; (iii) imutabilidade, pois os dados inseridos não podem ser alterados e (iv) ausência de intermediários, já que a existência de um terceiro garantidor é desnecessária (RAMOS; SILVA, 2019). Com essas características, serviços baseados em *blockchain* possuem grande utilidade para a promoção de transparência na Administração, para o combate à corrupção, para a participação popular em iniciativas de democracia digital. Isto pois a *blockchain* permite a criação de registros visíveis, imutáveis e confiáveis, impedindo o Estado de omitir informações de interesse público ou de alterar registros de forma arbitrária.

Algumas das aplicações mais comuns para a Administração Pública tem sido, por exemplo, a criação de contratos inteligentes, a modernização de registros de propriedade, o estabelecimento de mecanismos para garantia de confiança em processos eleitorais, a criação de sistemas de identidade digital, entre outros (RAMOS; SILVA, 2019). Fato é que a tecnologia *blockchain* ainda é uma invenção recente, sendo novos usos descobertos a cada dia. Porém, é importante ter atenção que algumas características das redes *blockchain* possuem interação complexa com as normas de proteção de dados pessoais.

Em primeiro, é preciso estabelecer que toda *blockchain* que contiver dados pessoais será objeto de regulação pelas leis de proteção de dados (MAKHDOOM et al., 2020), como a LGPD e o GDPR. Nestes casos, a ampla transparência e a imutabilidade das informações podem gerar tensão, por exemplo, com o direito à intimidade e com o direito à correção de dados tratados de forma inexata, já que o titular de dados não conseguirá apagar nem corrigir a informação pessoal disponível ao público (CHANG; ALMEIDA, 2020).

Ramos e Silva (2019) afirmam que, ao usar *blockchain* em cidades inteligentes, a Administração Pública deve implementar (e exigir que os atores privados implementem) boas práticas capazes de tornar mais harmônica a interação entre a tecnologia e as leis de proteção de dados. Para isso, é preciso identificar quando uma rede *blockchain* será pública (acessível a todos sem controle prévio), permissionada (possui limitações de visibilidade e registro de dados de acordo com o administrador) ou privada (de controle centralizado).

A *blockchain* privada pouco difere de uma base de dados comum, sendo incontroversa sua regulação pela lei. Contudo, as redes permissionadas e públicas devem ser implementadas com cuidado. Por tratar-se de tecnologia inovadora, a *blockchain* justifica a elaboração de avaliação de impacto (RIPD) para a delimitação de riscos e de medidas de mitigação. Diante dos riscos detectados na avaliação, o administrador da cidade inteligente poderá verificar se uma rede *blockchain* é realmente necessária para a operação desejada. Isto deve ocorrer especialmente diante de sua modalidade pública, já que a *blockchain* permissionada permite a implementação de salvaguardas, o que é impossível em uma *blockchain* pública (RAMOS; SILVA, 2019).

Além disso, o administrador urbano deve ter cuidado com a forma escolhida para armazenar os dados, tendo atenção ao princípio da minimização, objetivando

guardar somente as informações estritamente necessárias para o projeto, além de definir prazos para eliminação destas. Nas redes *blockchain,* isto ainda é um desafio, diante da relativa imutabilidade dos registros, o que demanda que o administrador tenha cuidado com qual tipo de informação irá inserir nos blocos, evitando, por exemplo, o tratamento de dados sensíveis. Tendo em mente a obrigação de avaliar a necessidade e a proporcionalidade de projetos de cidade inteligente baseados em *blockchain*, torna-se ainda mais evidente a obrigatoriedade de elaboração de RIPD, já que o relatório pode concluir que uma *blockchain* não é necessária ou oportuna (RAMOS; SILVA, 2019).

Uma abordagem cautelosa diante da *blockchain* é a melhor maneira de extrair as suas potencialidades de forma segura para a privacidade, rejeitando a opinião de que a tecnologia é uma panaceia que deve ser implementada de forma ampla em todos os setores de cidade inteligente. O administrador deve ter em mente, então, que diante de dúvida sobre a segurança ou oportunidade da implementação de *blockchain*, este deve priorizar outras soluções que estejam em consonância com as normas legais.

Conforme mencionado acima, além da aplicação de *blockchain* na arquitetura de serviços públicos com finalidade de garantir maior eficiência, rapidez ou transparência, existem protocolos de *blockchain* que atuam para garantir a segurança informacional e a proteção de dados pessoais. Por exemplo, pesquisadores elaboraram estratégias baseadas em *blockchain* para permitir o compartilhamento seguro de informações entre objetos dotados de IoT.

Isto é possível porque redes *blockchain* são capazes de manter a integridade da informação ao longo do compartilhamento, além de permitirem a utilização de validações automáticas de operações (a partir de características de contratos inteligentes). Assim, a tecnologia *blockchain*, apesar de possuir aplicações de maior risco, também possui capacidade de atuar como PET, potencializando a segurança e privacidade de dispositivos inteligentes (MAKHDOOM et al., 2020).

Outra característica que permite a aplicação de *blockchain* para a potencialização da segurança das cidades inteligentes é sua utilidade para o estabelecimento de protocolos de interoperabilidade. A maioria dos dispositivos de IoT operam em protocolos de comunicação vulneráveis e incapazes de interagir de forma compatível entre si. Hoje em dia, já é possível utilizar tecnologia *blockchain* para permitir que aparelhos dotados de IoT consigam interagir sem pôr em risco a

integridade a informação. Tal potencialidade é explorada por projetos como o *SmartLog*, na União Europeia, que permite que empresas do setor de transportes e logística utilizem uma *blockchain* pública para compartilhar e registrar informações sobre o fluxo transfronteiriço de mercadoria, o que é feito de forma segura e anonimizada (QI et al., 2017).

Como se vê, são muitas as possibilidades de uso de *blockchain* nas cidades inteligentes, o que torna a presente exposição limitada e sob o evidente risco de se tornar datada. Contudo, em linhas gerais, é possível afirmar que, se aplicada de forma cautelosa e estudada, as redes *blockchain* são uma valiosa adição para o urbanismo inteligente, podendo aproximar o cidadão da administração pública e potencializar a confiança. Por outro lado, o uso exagerado ou inconsequente da tecnologia pode causar o efeito reverso, vulnerabilizando o direito à proteção de dados e acabando por afastar o cidadão das iniciativas baseadas em *blockchain*.

4.6. Proteção de dados como elemento do direito à cidade

O direito, assim como a cultura, se altera com o passar do tempo, com a mudança dos costumes e com a evolução tecnológica. Nesse processo, é natural que garantias surjam e desapareçam e que direitos tenham seu âmbito de incidência expandido ou reduzido. Tendo isso em vista, o já mencionado direito à cidade passa por um processo de relocalização de sua influência, tendo a necessidade de incluir novos conteúdos não pensados pelas suas concepções originárias, como a de Henri Lefebvre.

O conteúdo do direito à cidade, em conexão com os projetos de cidade inteligente, se desdobra em um *direito à cidade inteligente,* cujas linhas gerais foram abordadas anteriormente (vide item 2.3). Tal garantia se mostra relevante ao buscar garantir que os cidadãos tenham o direito de se informar sobre como é construída a cidade inteligente e de se opor às visões autoritárias e tecnocráticas de convivência urbana. Diversas críticas podem ser tecidas à forma como a maioria das cidades inteligentes são desenhadas no presente.

Os três principais desafios éticos no que diz respeito às cidades inteligentes são: (i) a abordagem verticalizada (*top down*) da maioria dos projetos, que, apesar de envolverem uma retórica baseada no protagonismo do cidadão, dificilmente dão a ele o poder de participar da elaboração da cidade; (ii) o protagonismo que

iniciativas voltadas à segurança pública assumem, o que pode exacerbar os mecanismos de controle social e (iii) a falta de clareza e de ferramentas para exercício de direitos relacionados ao tratamento de dados pessoais dos cidadãos (GALIC; SCHUILENBURG, 2021).

Breuer e Pierson (2021) alegam que projetos de cidade inteligente somente irão promover a participação cidadã na medida em que esta for economicamente viável para os controladores de dados. Ou seja, em geral os cidadãos são vistos como consumidores ou usuários que consomem soluções prontas e oferecidas na cidade, sem participar do desenho destes projetos. A alienação do cidadão do processo de construção da cidade foi o que levou Lefebvre a imaginar um direito à cidade que vai além das condições materiais de habitação, incluindo também o direito que o cidadão tem de imaginar a cidade e influenciar em sua criação.

O conceito de cidadania, inaugurado por Aristóteles e desenvolvido pelas revoluções iluministas, hoje se vincula aos estudos sobre direitos fundamentais, sendo impossível pensar o direito à cidade sem entendê-lo como uma garantia que deve ser estendida a todos os seres humanos. Entendendo a cidade como um espelho da sociedade, Lefebvre entendia que a cidadania deveria garantir uma vida social mais justa e democrática, sendo os cidadãos capazes de influenciar no ambiente em que vivem (ALDINHAS FERREIRA, 2021).

O direito à cidade não propõe que o cidadão seja incluído em uma estrutura social já existente, mas que a cidade seja democratizada de modo a permitir que o cidadão participe dos processos de tomada de decisão. Em suma, é um direito pensado para criar um urbanismo centralizado na pessoa humana, buscando o seu empoderamento no ambiente urbano (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018). Contudo, as dimensões que impactam a cidadania no presente são distintas do contexto da década de 1960, quando a computação era embrionária e os métodos de processamento de informação eram muito mais básicos do que os atuais. Logo, falar em empoderar o cidadão urbano, hoje, requer uma discussão profunda sobre privacidade e proteção de dados.

Mesmo não tendo convivido com a internet como conhecemos[41], Lefebvre acreditava que a tecnologia poderia ser utilizada para melhorar a qualidade de vida nas cidades. Ainda assim, alertava para o risco de uma concentração de poder capaz

[41] Lefebvre faleceu no ano de 1991, mesmo ano em que foi publicada a primeira webpage na internet.

de utilizar a tecnologia para mascarar propósitos menos evidentes (SHAW; GRAHAM, 2020). É o que pode ocorrer em projetos verticalizados de cidade, conforme exposto ao longo do trabalho. Nas cidades inteligentes, os cidadãos tem pouca visibilidade sobre como e para que seus dados pessoais são tratados, assim sendo incapazes de questionar e alterar tais atividades de tratamento (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018).

Logo, além dos impactos na participação do cidadão na definição dos rumos da cidade, o direito à cidade contemporâneo precisa comportar questões relativas à proteção dos dados desses cidadãos. Para usufruir e influenciar a cidade no século XXI, é necessário que o cidadão esteja empoderado para garantir a sua intimidade, a sua autodeterminação informativa e os seus direitos enquanto titular de dados. Shaw e Graham (2020, p. 61) afirmam:

> Assumindo que a população urbana global hoje tem mais acesso à informação do que jamais registrado e, ainda assim a injustiça urbana persiste em escala massiva, alegamos que o elemento informacional do direito à cidade é um aspecto mais complexo da luta política do que Lefebvre era capaz de perceber à sua época. Isso pode ter ocorrido em razão do poder que os Estados possuíam à época de seus escritos ou por causa do fato menos previsível de que os cidadãos deixariam de ser simples consumidores de informação digital para tornarem-se produtores desta – em quantidades massivas[42].

Em sua concepção original, o direito à cidade era incapaz de ver que, no futuro, as cidades seriam capazes de mapear nossa localização, registrar nossos hábitos e utilizar todos esses dados coletados para diversas finalidades. Esse fenômeno é chamado de urbanização da informação, levando à consequência de que, para entendermos o direito à cidade, precisamos entender o espaço urbano como um espaço que também é informacional e marcado por intensos fluxos de informação digital que contém dados pessoais. Por isso, impõe-se uma nova leitura do direito à cidade que seja capaz de interpretar este espaço urbano que se produz e reproduz na esfera digital (SHAW; GRAHAM, 2020).

---

[42] "Given that the world's urban population now has more access to information than ever before, and yet urban injustice persists en masse, we contend that information's complement to a right to the city is now a more complex aspect of political struggle than Lefebvre could perhaps realize at the time. This may have been due to the relative power of state actors at the time of his writing (Lefebvre, 2014a: 810, 1991: 285), or because of the less imaginable fact that citizens would one day not simple consume digital information but also come to produce it themselves – and in huge quantities (Lefebvre, 2014b)". Tradução livre.

As máximas do direito à cidade, que objetivam a reapropriação do espaço, a participação popular e a auto-organização da sociedade, devem ser estendidas ao digital, permitindo que o habitante urbano tenha, cada vez mais, a capacidade de gerir como a sua informação flui pela cidade. Essa visão se relaciona com o conceito de soberania tecnológica, uma nova forma de cidadania que entende que a tecnologia deve ser orientada para servir os cidadãos locais, sendo usada como um bem comum e construído de forma coletiva e transparente (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018).

O direito à cidade foi criado para se opor à concentração de poder - político e econômico - que levava as cidades a serem orientadas e usufruídas de forma desigual pelos cidadãos. Na *smart city*, as forças mudam de natureza, adquirindo um caráter informacional representado pela assimetria entre controladores e titulares de dados. Enquanto os primeiros tem amplo acesso a dados sobre os cidadãos, conhecendo seus hábitos e suas características, o titular de dados possui poucos detalhes sobre quais dados estão sendo coletados, de que forma estes são tratados e como fazer para exercer direitos (ZUBOFF, 2018).

Esse poder agregado significa que os detentores da tecnologia são capazes de produzir e interpretar a informação que irá determinar os rumos do planejamento urbano. Trata-se de uma lógica que se retroalimenta: os detentores da tecnologia reduzem a cidade a um conjunto de informações e reintroduzem essas informações para influenciar o planejamento urbano (SHAW; GRAHAM, 2020). Nessa assimetria de direitos de privacidade, em que controladores sabem muito sobre titulares que estão destituídos de informação, colabora para que a cidade seja construída de forma padronizada e pouco participativa. Atinge-se, a partir da análise de dados, uma espécie de consenso tecnológico sobre quais são as melhores soluções, devendo o cidadão somente consumi-las.

Isso pode vir a causar danos a uma das dimensões do direito à cidade, que é o direito de divergir de projetos uniformizantes de cidade. Essa ausência de conflito de posições divergentes e falta de oportunidade para questionamento das soluções adotadas pode desestimular a participação política e afetar a democracia nas cidades (GALIC; SCHUILENBURG, 2021). Assim, Lefebvre defendia que os encontros entre posições divergentes deve ser um dos atrativos da cidade, atuando como força motriz de seu desenvolvimento mais justo.

A discordância é entendida, desde Maquiavel, como uma das principais fundações da democracia, já que permite o conflito entre posições até a chegada a uma solução ideal[43]. O cidadão precisa ser capaz de discordar dos rumos que a cidade toma, o que depende da promoção de abertura, participação e representatividade nas cidades inteligentes (SHAW; GRAHAM, 2020). Por isso, as já mencionadas iniciativas colaborativas e abertas são essenciais para a promoção do dissenso democrático nas cidades, permitindo o reequilíbrio dos direitos de proteção de dados e a criação de uma *smart city* focada no cidadão (KITCHIN; CARDULLO; DI FELICIANTONIO, 2018).

O posicionamento dos cidadãos como tomadores de decisão no planejamento urbano possui paralelos com as legislações mais modernas de proteção de dados, como o GDPR e a LGPD, que objetivam fornecer ferramentas para que o titular de dados possa determinar como se relacionar com a tecnologia. Enquanto Lefebvre buscava equipar o cidadão para que este pudesse se empoderar diante do urbanismo tradicional, tornando-o peça central do planejamento urbano, as legislações de proteção de dados caracterizam a pessoa humana como centro do regime legal, devendo ser capaz de realizar a autogestão de suas informações e ter mecanismos para exigir seus direitos (BREUER; PIERSON, 2021).

Neste ponto, é evidente a conexão dessas leis com os direitos humanos e fundamentais que constroem o direito à cidade:

> Na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) adotado em 2016 regula o tratamento de proteção de dados em combinação com direitos e liberdades fundamentais garantidos em outros documentos (Hallinan & Martin, 2020). A ênfase do GDPR nos 'titulares de dados' sugere interseções entre direitos de proteção de dados e o envolvimento significativo dos cidadãos no processo socio-tecnológico que cria cidades (inteligentes), como determinado pelo direito à cidade (BREUER; PIERSON, 2021, p. 801).[44]

O ferramental de leis como o GDPR e a LGPD é imprescindível para que consigamos desenhar serviços de cidade inteligente que tenham o cidadão como

[43] "(...) os bons exemplos nascem da boa educação; a boa educação, das boas leis; e as boas leis, dos tumultos que muitos condenam sem ponderar" (MAQUIAVEL, 2007, p. 22)

[44] "In the European Union, the General Data Protection Regulation (GDPR) adopted in 2016 regulates processing of personal data in combination with fundamental rights and freedoms enshrined in other documents (Hallinan & Martin, 2020). The GDPR's emphasis on 'data subjects' suggests intersections between rights to data protection and meaningful involvement of citizens in the socio-technological processes that make up (smart) cities, as suggested by the right to the city". Tradução livre.

foco, o que nos leva a sugerir que a proteção de dados tenha se tornado conteúdo essencial do direito à cidade. Contudo, essas normas devem ser interpretadas de acordo com a visão de que a proteção de dados supera a mera individualidade, devendo ser entendida, como ensina Rodotà (2007), como uma questão coletiva de relevância social, política e econômica (DONEDA; BELLI, 2021).

O controle individual de processos massivos de tratamento de dados, como os que ocorrem nas cidades inteligentes, é extremamente dificultoso, seja por dificuldades operacionais ou pela falta de interesse na promoção da responsabilização e transparência. Ainda, é possível que a implementação dessas normas venha a dar margem para que controladores forneçam pouca informação sobre seus projetos, haja vista seu poder decisório e as amplas garantias de segredo industrial e comercial (BREUER; PIERSON, 2021).

A promoção da participação popular e a garantia dos direitos de proteção de dados deve, então, suplantar o mero formalismo e o atendimento individual das demandas de titulares. Conceitos jurídicos não devem somente promover uma nova visão sobre a realidade, mas permitir a criação de uma nova realidade a partir de mecanismos concretos de atuação (SHAW; GRAHAM, 2020), o que impõe que os atores de cidades inteligentes promovam a participação e o diálogo desde a concepção dos projetos.

Para que essa participação seja eficiente, a sociedade precisa ser capaz de compreender a dinâmica de tratamento de dados nas cidades, o que requer investimento em conscientização. Ademais, o direito à cidade enfrenta outros dois grandes obstáculos. Em primeiro, a participação popular dificulta a tomada de decisões, o que se traduz em aumento de custos e em uma necessidade de envolvimento de parcelas diferentes da população para garantia de representatividade. Em segundo, as legislações de proteção de dados, apesar dos avanços, ainda não estão plenamente equipadas para dimensão coletiva das cidades inteligentes, dando aos controladores amplo poder decisório e estando despidas de mecanismos de participação coletiva (BREUER; PIERSON, 2021).

Em conclusão, já percorremos parte do caminho para que seja possível incluir a proteção de dados como um conteúdo do direito à cidade, mas ainda estamos aquém do necessário para que este de fato se materialize. Para isso, será necessário que surjam novas normas que adequem o regime de proteção de dados ao fenômeno único que é o tratamento de dados pessoais em cidades inteligentes.

Diante da lacuna legal, corremos o risco de que o chamado direito à cidade inteligentes seja inefetivo, pensado de maneira individualizada e formalística. Tal lacuna pode ser preenchida pela ANPD, a partir de regulações que promovam a transparência, a soberania tecnológica, a participação popular, o *privacy by design* e outros conceitos capazes de dar ao titular de dados e à sociedade civil maior protagonismo nas cidades inteligentes.

5. Considerações Finais

> (...) a cidade é um lugar complexo, o que significa que é cheio de contradições e ambiguidades. A complexidade enriquece a experiência; a clareza a empobrece (SENNET, 2021, p. 17)

Na célebre obra "As cidades invisíveis", Italo Calvino (1990) utiliza as cidades como alegoria para tratar de temas como o amor, a cobiça, a morte, o trabalho, a guerra e a paz. Ao encenar conversas entre o viajante Marco Polo e o imperador mongol Kublai Khan, o escritor descreve como as cidades refletem, de maneiras diversas, a forma como vivem os seres humanos. Ao falar das cidades, o autor fala dos humanos e, descrevendo os humanos, atinge o que quer dizer sobre as cidades. Calvino entende as cidades como o palco da vida, o local onde a humanidade se cria e se reinventa e que pode ser pensado de diversas maneira, algumas melhores que outras.

O debate entre viajante e imperador ilustra como os impasses que enfrentamos com as cidades inteligentes, ainda que novos em conteúdo, são antigos em formato. Estamos diante, ainda, do conflito do urbanismo autoritário com a construção dialógica da cidade. Enquanto o imperador está em busca da cidade perfeita, que pode ser construída segundo sua mente, o viajante responde:

> (...) As cidades, como os sonhos, são construídas por desejos e medos, ainda que o fio condutor de seu discurso seja secreto (...) As cidades também acreditam ser obra da mente ou do acaso, mas nem um nem o outro bastam para sustentar as suas muralhas. De uma cidade, não aproveitamos as suas sete ou setenta e sete maravilhas, mas a resposta que dá às nossas perguntas (CALVINO, 1990, p. 20).

O diálogo traz o desafio que é equilibrar a construção de cidades com a resolução dos problemas de seus habitantes. As cidades inteligentes, hoje, apesar de parecerem "obra da mente" gerada de forma objetiva com as melhores tecnologias, possuem um discurso cujo "fio condutor é secreto". Estas cidades, pensadas em parceria com atores envolvidos na economia movida a dados, se inserem em uma lógica de extração de dados e pouca participação dos cidadãos em seu desenho. Então, por mais que se propague a *smart city* como resposta, o modelo hegemônico não está efetivamente respondendo às perguntas da população. Como resultado, ainda estamos distantes de aproveitarmos suas "maravilhas".

Buscando entender que “medos e desejos” compõem a cidade, o presente trabalho contrapõe o “discurso secreto” da cidade vigiada a uma visão esperançosa de que podemos mitigar a violação à privacidade dos cidadãos. Para isso, buscou-se entender como é a relação entre a cidade inteligente, em suas múltiplas acepções, e a privacidade, conceito que também se multiplica e evolui ao longo do tempo, desdobrando-se no direito à proteção de dados. Ambos os temas tratam de fenômenos antigos: a separação entre público e privado e a organização do espaço público urbano. Ainda assim, inovações tecnológicas recentes adicionam componentes que merecem cuidadoso estudo.

Voltando a Calvino, a cena retratada simboliza que cidades podem ser construídas de formas autoritárias ou dialógicas. A dinâmica da construção de uma cidade é desafiadora: os motores do progresso não tem paciência, mas, ao mesmo tempo, as mudanças impactam diretamente na vida dos habitantes, que deveriam ter o direito de se manifestar de forma livre. Richard Sennet (2021) entende que um dos principais defeitos que um projeto urbanístico pode ter é adotar uma abordagem fechada. Hausmann e Le Corbusier, ao delimitarem, prévia e objetivamente, que forma deve ter a cidade ideal, são exemplos disso.

Hoje, as cidades inteligentes são, em sua maioria, projetos fechados. Estas são pensadas de acordo com a teoria de sistemas, sendo fatiadas em um número de dimensões, como a mobilidade e a sustentabilidade, que podem ser melhoradas a partir de soluções adotadas em série (SÖDERSTROM et al., 2014). Estes sistemas, que são aplicados para cidades de realidades distintas, geralmente dependem de IoT, *big data* e computação em nuvem, tecnologias que dificultam a harmonização da cidade com a proteção de dados (EDWARDS, 2016). Ainda, além do apetite por dados, o funcionamento da cidade inteligente é obscuro, dependendo de algoritmos proprietários, de bases de dados controladas por variados agentes e de uma estrutura de governança ainda deficiente.

O problema é que ainda estamos distantes de um formato que permita a participação do cidadão no processo de construção. As cidades inteligentes são “fechadas” porque existe pouco estímulo, do Estado e do mercado, para que se questionem parcerias que movimentam somas significativas de dados e recursos. Colocar em dúvida a cidade inteligente significa também colocar em dúvida parcerias público-privadas desejadas por administradores que se encontram despidos de recursos e por empresas que querem expandir seu portifólio de clientes

(MOROZOV; BRIA, 2019). Além disso, questionar a retórica hegemônica da cidade inteligente impõe o questionamento da lógica econômica contemporânea, baseada na troca de dados pessoais por serviços (ZUBOFF, 2021). Isto pois esse consolidado processo se transferiu para as cidades, sendo o cidadão um consumidor de soluções prontas e um produtor de dados que serão processados.

Entretanto, por mais dolorosa que seja a realização da crítica, ela é o caminho para que as cidades inteligentes atinjam a sua promessa de solução de problemas urbanos a partir da tecnologia. A suposta troca, em que damos a nossa privacidade em troca de melhores serviços, não é verdadeira. Nossos dados são inseridos em um sistema econômico que os vê como uma peça em uma engrenagem econômica, buscando retirar deles a solução viável mais lucrativa. E isto nem sempre significa atingir a solução que mais se adeque ao problema abordado e à realidade local (MOROZOV, 2018). Por exemplo, empresas privadas buscam maximizar os seus ganhos e dificilmente irão ceder, em parcerias com as administrações, dados que vão contra as suas intenções[45].

Não se trata de adotar uma abordagem contrária ao setor privado. É natural que este defenda seus interesses e busque maximizar seus lucros e devemos lembrar que a maioria das aplicações utilizadas na cidade inteligente foram desenvolvidas pelo setor privado, que deve ser entendido como um ator essencial neste processo. Por outro lado, cabe à sociedade o papel de questionar de que forma as empresas agem nas cidades inteligentes, assim como cabe ao Poder Público implementar as leis de proteção de dados, tanto em sua atuação quanto na atuação das empresas. Esse tensionamento entre os polos deve ser entendido como positivo, podendo a sociedade, o Estado e o mercado debaterem a melhor forma de equacionar a "inteligência" das cidades com a proteção de dados pessoais.

É com este sentido que Kitchin, Cardullo e Di Feliciantonio (2018) entendem que o direito à cidade é uma forma de reinserir a política no debate sobre cidades inteligentes, permitindo o embate entre versões conflitantes de urbanismo. Tanto o Estado quanto o mercado devem aceitar o debate com os cidadãos, haja vista que serão esses os maiores afetados pela eventual má condução de projetos

[45] Morozov (2018) cita, por exemplo, a crescente dependência que cidades estadunidenses possuem de dados fornecidos por aplicativos de transporte. Estes são cedidos para cidades, como Boston, que os reutiliza para definir suas políticas públicas de mobilidade. Contudo, segundo o autor, estes dados representam uma realidade mapeada segundo o critério desejado por estas empresas, dando a elas ainda mais poder de influenciar o processo político.

urbanos. A população deve ser ouvida para entendermos se a cidade deve priorizar, por exemplo, a utilização de reconhecimento facial ou uma rede inteligente de energia. Afinal, não existe critério objetivo para definir qual é o melhor modelo de cidade, devendo este ser definido de forma coletiva.

Contra o citado urbanismo fechado, Sennet (2021) contrapõe a visão da cidade aberta, capaz de comportar as tensões, o debate e o imprevisível. Para o autor, o pensar aberto permite maior flexibilidade em sistemas complexos como as cidades, repletas de variáveis que se interrelacionam. Considerando que "*a complexidade enriquece a experiência; a clareza a empobrece* (2021, p. 17), Sennet remonta a Aristóteles para defender que as melhores formas de governar a cidade sempre foram aquelas capazes de comportar diferentes visões de mundo.

Pensando a cidade inteligente, é possível verificar que, tanto a internet como a cidade, podem ser abordadas de maneiras mais abertas ou mais fechadas. Enquanto a utopia da internet a pensava como uma grande aldeia global, horizontalizada e transparente, hoje os sistemas digitais se assemelham a caixas-pretas, sendo regidos por algoritmos proprietários obscuros (FRAZÃO, 2020). Ocorre que, no presente, a retórica da cidade inteligente parece combinar abordagens fechadas que se dão nas esferas do urbanismo e dos serviços digitais.

Em razão disso, Sennet (2021) contrapõe dois modelos de cidade inteligente. O primeiro é o modelo prescritivo, baseado em uma política de controle centralizado, em algoritmos proprietários, na coleta unilateral de dados e na rejeição à participação popular e à transparência, representando um pensar fechado que adota soluções prontas. Em contraponto, o autor propõe a cidade inteligente coordenativa, que não tem medo da fricção que pode ser causada pela discordância entre as partes, promovendo a transparência e o debate. Neste modelo aberto, em vez de optarmos entre opções de sistemas prontos, a tecnologia é utilizada para dar ao cidadão o direito de escolher como abordar os problemas.

O pensamento aberto não diz respeito somente aos serviços e como esses serão implementados. A cidade inteligente coordenativa se alia ao ideal da autodeterminação informacional, já que os dados colhidos são utilizados para finalidades que a população conhece e escolhe, além de serem processados por algoritmos que ela é capaz de entender. Enquanto em uma cidade prescritiva os dados são colhidos de forma verticalizada, processados de forma pouco transparente e reaproveitados em soluções encaixotadas, a cidade coordenativa

obriga o cidadão a "*se envolver com os dados, interpretando-os (...) e agindo de acordo com eles, para melhor e para pior – pois uma cidade inteligente cooperativa pode cometer erros*" (SENNET, 2021, p. 192).

Este direito de errar contraria a visão de que a cidade deve obedecer a um tipo ideal estático, podendo comportar o imprevisível e o conflitante e tornar-se mais resiliente (HILLER; BLANKE, 2017). Apesar de tal modelo ainda ser de difícil organização, existem iniciativas que demonstram que a cidade inteligente coordenativa não é uma utopia. Sennet (2021) traz o exemplo do orçamento participativo, sistema criado em 1989 em Porto Alegre (RS) para dar aos cidadãos a capacidade de debater e opinar sobre a distribuição de recursos públicos, sendo evidência da política urbana sendo feita de baixo para cima.

O autor argumenta que, como a participação virtual nunca foi mais fácil, a tecnologia pode ser usada para dar voz aos cidadãos, possibilitando sua atuação até nas megacidades. A valorização do cidadão e dos seus dados pessoais é um passo necessário para que esse possa contribuir com a cidade inteligente e torná-la mais receptiva aos problemas concretos de cada local. Por este motivo, a cidade que permite o envio de *feedbacks* por parte da população efetiva a democracia e a soberania digital (MOROZOV; BRIA, 2019).

Já existem projetos que buscam promover o uso responsável de dados pessoais e a democracia nas cidades inteligentes. Em verdade, esses objetivos andam juntos, pois a falta de transparência viola tanto a privacidade quanto a participação dos cidadãos na esfera pública (ZUBOFF, 2018). Neste sentido, se destaca a cidade de Barcelona, cujo modelo de *smart city* é pautado na participação, na adoção de sistemas *open source* e na promoção da transparência no uso de dados (MOROZOV; BRIA, 2019). Como exemplo de cidade inteligente prescritiva, podemos citar a cidade sul-coreana de Songdo e Masdar, na Arábia Saudita, cujos projetos foram realizados sem participação popular e com evidente dependência de empresas de tecnologia (SENNET, 2021).

Como se vê, a cidade inteligente não é boa nem má por si só. Em verdade, sequer sabemos com precisão o que ela é, mas precisamos saber o que queremos delas. Voltando à Calvino, se é a cidade deve responder às nossas perguntas, é necessário que essas perguntas sejam feitas e que o cidadão tenha como expressar suas preocupações. Sendo assim, não trouxemos respostas, mas dúvidas, já que,

mais do que um projeto pronto, a cidade inteligente deve ser entendida como um processo contínuo de construção que contém diversas trajetórias possíveis.

Deste modo, a presente pesquisa realizou, em primeiro, a seguinte pergunta: o que é, afinal, uma cidade inteligente? Concluiu-se que a resposta definitiva excede o escopo deste trabalho, cujo foco é a privacidade e proteção de dados pessoais no ambiente urbano. Ainda assim, foi possível entender que as cidades inteligentes são, mais do que um caminho evidente a um progresso técnico e objetivo, uma escolha política que pode ser feita de diversas maneiras.

A *smart city* é mais um componente dentre um amplo processo que é a utilização de dados pessoais como matéria de um novo sistema econômico. Além de serem parte da economia movida a dados, estes projetos também replicam características essenciais do urbanismo progressista, baseado em tipos ideais de cidade pautados em racionalidades supostamente objetivas. Por fim, foram mapeadas as principais características tecnológicas das cidades inteligentes, que dependem de invenções cuja relação com a proteção de dados pessoais é tensa.

O terceiro capítulo faz as seguintes perguntas: como a cidade inteligente se relaciona com a proteção de dados e a segurança da informação? Responder a essa pergunta exigiu que se investigasse como a privacidade ocorre em espaços públicos, permitindo a conclusão de que, hoje, a fronteira entre público e privado é porosa e oscilante. Isto faz com que os cidadãos estejam produzindo e enviando dados tanto em ambientes privados como públicos, trazendo novos desafios no que diz respeito à quantidade de dados enviados, à finalidade de tratamento, à transparência e à qualidade dos dados. Ademais, a estrutura complexa das cidades produz diversas camadas tecnológicas que podem se expor a ataques cibernéticos, o que requer especial atenção com a segurança das informações nela tratadas.

No contexto brasileiro, a resposta à segunda pergunta perpassa obrigatoriamente pela LGPD. Sendo assim, foram explicados os princípios da lei e os principais direitos aplicáveis à realidade das cidades inteligentes. Estes valores buscam limitar o tratamento de dados em finalidade, escala e duração, além de impor a realização de mecanismos de transparência. Ademais, os princípios da LGPD obrigam que os controladores adotem medidas de segurança da informação e que se responsabilizem por eventuais consequências adversas. Nenhum dos princípios elencados é de fácil aplicação no ambiente complexo das cidades, mas a

presença de um regime legal estruturado nos permite ter um norte, cuja efetivação irá depender, também, de uma postura ativa por parte da ANPD.

Por fim, a terceira pergunta é a mais difícil. Afinal, como equacionar inteligência urbana e privacidade? Seria isto possível? Em linha com Martínez-Ballesté et al. (2013), acreditamos que sim, é possível que a cidade inteligente respeite a privacidade dos cidadãos. Isto irá depender, conforme exposto, de soluções tecnológicas e jurídicas, o que requer diálogo multissetorial intenso entre o regulador e os pesquisadores das mais diversas áreas.

O presente trabalho, em razão da linha de pesquisa, priorizou a exposição de mecanismos jurídicos e organizacionais, como a implementação de obrigações da LGPD, a nomeação de encarregado de dados, a promoção da confiança do cidadão e da transparência e a defesa do direito à cidade. Ainda assim, foram estudadas soluções tecnológicas, como a tecnologia *blockchain,* os projetos de dados abertos e de transparência algorítmica. Além disso, foram abordadas as PETs, peça essencial na promoção do *privacy by design*.

Conforme exposto, a regulação da tecnologia e das cidades são fenômenos que podem ser abordados a partir de diversos prismas. Optou-se por direcionar a abordagem da cidade inteligente sob o prisma da proteção de dados pessoais, com forte influência das normas da LGPD e do GDPR. Naturalmente, esta abordagem não pretende ser totalizante e abordou temas complexos que demandarão aprofundamento da pesquisa. Entretanto, apesar das limitações, o trabalho serve como ponto de partida para entendermos a relação entre cidade e proteção de dados.

Como forma de complementação ao estudo, alguns possíveis direcionamentos futuros são: (i) o estudo de aplicações tecnológicas concretas e de como se dá a adequação destas a legislação; (ii) o estudo de exemplos concretos de cidade inteligente para verificar o impacto sobre a proteção de dados; (iii) o aprofundamento no estudo do direito urbanístico para permitir verificar a sua interação com as normas de proteção de dados e (iv) a aproximação da pesquisa jurídica com a pesquisa urbanística, para trazer maior rigor à abordagem do fenômeno urbano.

REFERÊNCIAS

ABREU, J. de S. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: DONEDA, D. et al., (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 583-604.

AHMED, K. B.; BOUHORMA, M.; AHMED, M.B. Age of Big Data and Smart Cities: Privacy Trade-Off. **International Journal of Engineering Trends and Technology (IJETT)**, v. 16, n. 6, out. 2014, p. 298-304.

ALDINHAS FERREIRA, M. I. The Right to the City: The Right to Live with Dignity. In: ALDINHAS FERREIRA, M. I. (ED.). **How Smart Is Your City?: Technological Innovation, Ethics and Inclusiveness**. Cham: Springer International Publishing, 2021. v. 98, p. 17-26

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.

ANPD. **Anpd Abre Inscrições Para Participação Em Reunião Técnica Sobre Relatório De Impacto De Proteção De Dados Pessoais**. Maio de 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-inscricoes-para-participacao-em-reuniao-tecnica-sobre-relatorio-de-impacto-de-protecao-de-dados-pessoais. Acesso em 3 de abril de 2022.

ANPD. **Abertas inscrições para tomada de subsídios sobre a norma do encarregado.** Março de 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/abertas-inscricoes-para-tomada-de-subsidios-sobre-a-norma-do-encarregado. Acesso em 3 de abril de 2022.

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.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro, 2006

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

BARTOLI, A. et al., **"Security and privacy in your smart city"** in Proc. Barcelona Smart Cities Congr., 2011, pp. 1–6.

BATTY, M. Does Big Data Lead to Smarter Cities?. **I/S: A journal of Law and Policy**, Vol. 11:1, 2015, p. 127-151

BENTHAM, J. **The Panopticon Writings**. London: Verso, 1995. p. 29-95

BIONI, B. R. Compreendendo o conceito de anonimização e dado anonimizado: In: DONEDA, D.; MENDES, L. S.; CUEVA, R. V. B. (coords.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018) - A caminho da efetividade:**

contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 39-54.

BIONI, B. R. **Proteção de Dados Pessoais: a função e os limites do consentimento.** 3ª edição. Rio de Janeiro: Forense, 2021

BOURDIEU, Pierre. **Sobre o Estado.** São Paulo: Companhia das Letras, 2014

BRAGA, C. Discriminação nas decisões por algoritmos: polícia preditiva. In: FRAZÃO, A.; MULHOLLAND, C. (coord.). **Inteligência Artificial e Direito. 2ª edição.** São Paulo: Thomson Reuters Brasil, 2020, p. 691-715.

BRASIL. **Carta Brasileira de Cidades Inteligentes**, 2019. Disponível em: https://www.gov.br/participamaisbrasil/carta-brasileira-para-cidades-inteligentes4. Acesso em 10 ago. 2021.

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.** Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

BRASIL. **Resolução CD/ANPD Nº 2, de 27 De Janeiro De 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial da União: edição 20, seção 1, p. 6, 2022.

BRAUN, T. et al. Security and privacy challenges in smart cities. **Sustainable Cities and Society**, v. 39, 2018, p. 499-507.

BREUER, J. et al.. Identifying GDPR enforcement problems and requirements in Smart Cities (D.1.6). **SPECTRE Research Project**, Bruxelas: FWO, s. d. Disponível em: https://spectreproject.be/. Acesso em 25 de março 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.

BREUER, J.; PIERSON, J. The right to the city and data protection for developing citizen-centric digital cities. **Information, Communication & Society,** v. 24, n. 6, p. 797–812, 26 abr. 2021.

BREUER, J.; VAN BRAKEL, R. Data subjects/citizens' privacy expectations in Smart Cities. **SPECTRE Research Project**, Bruxelas: FWO, s. d. Disponível em: https://spectreproject.be/. Acesso em 3 de abril de 2022.

BRUNO, M. G. da S. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. In: MALDONADO, V. N.; OPICE BLUM, R. (coord.). **Lei Geral de Proteção de Dados Comentada.** 2ª edição. São Paulo: Thomson Reuters Brasil, 2010, p. 309-332.

CALVINO, I. **As cidades invisíveis.** São Paulo: Companhia das Letras, 1990.

CARDOSO, B. Estado, tecnologias de segurança e normatividade neoliberal. In: BRUNO, F. et al. (eds.). **Tecnopolíticas da vigilância: perspectivas da margem**. 1a edição ed. São Paulo, SP: Boitempo, 2018, p. 91-106.

CHANG, A.; ALMEIDA, C. B. D. Blockchain e Proteção de Dados. In: PALHARES, F. (coord). **Temas Atuais de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020, p. 100-126

CHINELLATO, S. J. A.; MORATO, A. C. Direitos básicos de proteção de dados pessoais, o princípio da transparência e a proteção dos direitos intelectuais. In: DONEDA, D. et al., (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 641-664.

CHOENNI, S. et al. Exploiting Big Data for Smart Government: Facing the Challenges. Em: AUGUSTO, J. C. (Ed.). . **Handbook of Smart Cities**. Cham: Springer International Publishing, 2021. p. 1035–1057.

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.

CISCO. **What is a Smart City?**. 2022. Disponível em: https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html. Acesso em 07 ago. 2021.

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

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

CITY OF SEATTLE. **Privacy Reviews of City Technology.** Seattle, WA: Seattle Information Technology, 2022b. Disponível em: https://www.seattle.gov/tech/initiatives/privacy/privacy-reviews. Acesso em 18 de Janeiro de 2022.

CUI, L.; XIE, G.; QU, Y.; LONGXIANG, G.; YANG, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. **IEEE Access – Special Section on Challenges and Opportunities of Big Data Against Cyber Crime**, Vol. 6, 2018, pp. 46.134-46.145

CURZON, J.; ALMEHMADI, A.; EL-KHATIB, K. A survey of privacy enhancing technologies for smart cities. **Pervasive and Mobile Computing**, v. 55, p. 76–95, abr. 2019.

DAS, A.; SHARMA, S. C. M.; RATHA, B. K. The New Era of Smart Cities, From the Perspective of the Internet of Things. In: RAWAT, D.B.; GHAFOOR, K. Z. **Smart cities cybersecurity and privacy**. 1st edition ed. Cambridge, MA: Elsevier, 2018, p. 1-9.

DAVIES, T. Shaping participatory public data infrastructure in the smart city: open data standards and the turn to transparency. In: WILLIS, K. S.; AURIGI, A.; ROUTLEDGE (FIRM) (EDS.). **The Routledge companion to smart cities.** New York: Routledge, 2020, p. 74-90.

DIMOV, D. **Lessons learned from the Fresenius ransomware cyberattack**. INFOSEC, 2020. Disponível em: https://resources.infosecinstitute.com/topic/lessons-learned-from-the-fresenius-ransomware-cyberattack/. Acesso em 30 de março 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.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. 2ª edição. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, D. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: DONEDA, D.; MENDES, L. S.; CUEVA, R. V. B. (coords.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018) - A caminho da efetividade: contribuições para a implementação da LGPD.** São Paulo: Thomson Reuters Brasil, 2020, p. 243-255

DONEDA, D. Panorama Histórico da Proteção de Dados Pessoais. In: In: DONEDA, D. et al., (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 3-20.

DONEDA, D.; MACHADO, D. **Cidades Inteligentes, Dados Pessoais e Direitos dos Cidadãos no Brasil**. CyberBRICS, 2019. Disponível em: https://cyberbrics.info/cidades-inteligentes-dados-pessoais-e-direitos-dos-cidadaos-no-brasil/. Acesso em 3 de abril de 2022.

DONEDA, D.; BELLI, L. Governança De Dados Nas "Cidades Inteligentes": Ensinamentos Aprendidos Das Práticas Brasileiras E Europeias. In: REIA, J.; BELLI, L. (org.) **Smart Cities no Brasil: regulação, tecnologia e direitos**. Belo Horizonte, MG: Casa do Direito, 2021, p. 61-81.

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 Electronic Journal, 2016.

EUROPEAN COMMISSION**. Proposal for a European Interoperability Framework for Smart Cities and Communities (EIF4SCC)**: final study report. Luxembourg: Publications Office of the European Union, 2021

EUROPEAN PARLIAMENT. Mapping the Smart Cities in the EU. **IP/A/ITRE/ST/2013-02 PE 507.480**, 2014. Disponível em: https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET%282014%29507480_EN.pdf. Acesso em 09 ago. 2021.

EVANS, L. The privacy parenthesis: Private and public spheres, smart cities and big data. In: COLETTA, C. et al.. **Creating Smart Cities.** Londres: Routledge, 2018, pp. 194-204

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.

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.

FIRMINO, R. J. Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. In: BRUNO, Fernanda, et al. **Tecnopolíticas da Vigilância – perspectivas da margem**. São Paulo: Boitempo, 2018

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 Lei Geral de Proteção de Dados. In: FRAZÃO, A.; DONATO OLIVA, M.; TEPEDINO, G. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 2ª edição. São Paulo: Thomson Reuters Brasil, 2020, p. 23-52.

GALATI, S. R. Funding a Smart City: From Concept to Actuality. In: MCCLELLAN, S.; JIMENEZ, J. A.; KOUTITAS, G. (Eds.). **Smart Cities**. Cham: Springer International Publishing, 2018. p. 17–39.

GALIČ, M.; SCHUILENBURG, M. Reclaiming the Smart City: Toward a New Right to the City. Em: AUGUSTO, J. C. (Ed.). . **Handbook of Smart Cities.** Cham: Springer International Publishing, 2021. p. 1419–1436.

GOVERNMENT OF INDIA. **DataSmart Cities: Empowering Cities through Data.** Nova Delhi: Ministry of Housing Affairs, 2018

GOVTECH. **Chief Data Officers: Which State and Local Governments Have a CDO?.** Julho, 2018. Disponível em: https://www.govtech.com/people/chief-data-officers-which-state-and-local-governments-have-a-cdo.html. Acesso em 3 de março de 2022.

GRAHAM, S. **Cities under siege: the new military urbanism**. Nova Iorque: Verso, 2011.

HALEGOUA, G. R. **Smart Cities.** Cambridge, MA: MIT Press, 2020

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

HILLER, J. S.; BLANKE, J. M. Smart Cities, Big Data, and the Resilience of Privacy. **Hastings Law Journal**, Vol. 68, Issue 2, 2017, p. 309-356

HUREL, L. M. Securitização E A Governança Da Segurança Cibernética No Brasil. In: SILVA, A. et al. **Horizonte Presente: tecnologia e a sociedade em debate.** Belo Horizonte: Casa do Direito. Fundação Getúlio Vargas, 2019, p. 320-343

IGNÁCIO, B. **Governo federal usa LGPD como pretexto para esconder dados, alertam especialistas**. Tecnoblog, 2022. Disponível em:

https://tecnoblog.net/especiais/governo-federal-esta-usando-lgpd-como-pretexto-para-esconder-dados/. Acesso em 5 de abril de 2022.

ISMAGILOVA, E. et al. Security, Privacy and Risks Within Smart Cities: **Literature Review and Development of a Smart City Interaction Framework**. Information Systems Frontiers, 21 jul. 2020.

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

ITCHRONICLES. **Top 5 Smart City Companies**. Setembro, 2021. Disponível em: https://itchronicles.com/smart-city/top-5-smart-city-companies/. Acesso em 19 de março de 2022.

JIMENE, C. D. V. Capítulo VII – Da Segurança e Das Boas Práticas. In: MALDONADO, V. N.; OPICE BLUM, R. (coord.). **Lei Geral de Proteção de Dados Comentada**. 2ª edição. São Paulo: Thomson Reuters Brasil, 2019, p. 333-360.

KHAN, Z.; PERVEZ, Z.; ABBASI, A. G. Towards a secure service provisioning framework in a Smart city environment. **Future Generation Computer Systems**, v. 77, p. 112–135, dez. 2017.

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

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. 2021.

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 ago. 2021.

KITCHIN, R. Urban science: prospect and critique. In: WILLIS, K. S.; AURIGI, A.; ROUTLEDGE (FIRM) (EDS.). **The Routledge companion to smart cities.** New York: Routledge, 2020, p. 61-73.

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

LAPSCHENK, A. de F.; FERREIRA, A. S.; CASTAGNA, A. G.; Carta Brasileira Para Cidades Inteligentes: Contexto E Conexões Com A Literatura. **Anais do I Seminário Internacional de Arquitetura e Urbanismo (SIAU) da Universidade do Oeste de Santa Catarina - Cidades inteligentes: tendências para o futuro**, Xanxerê: UNOESC, 2021

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

LEFEBVRE, H. **O direito à cidade**. São Paulo: Centauro, 2001.

LEMKE, T. **Biopolitics: an advanced introduction.** New York: New York University Press, 2011.

LEMOS, R.; BRANCO, S. Privacy by Design: conceito, fundamentos e aplicabilidade na LGPD. In: In: DONEDA, D. et al., (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 447-457

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 edição ed. Rio de Janeiro, RJ, Brasil: FGV Editora, 2018.

MAKHDOOM, I. et al. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. **Computers & Security**, v. 88, p. 101653, jan. 2020.

MALDONADO, V. N.; Capítulo III – Dos Direitos do Titular. In: MALDONADO, V. N.; OPICE BLUM, R. (coord.). **Lei Geral de Proteção de Dados Comentada.** 2ª edição. São Paulo: Thomson Reuters Brasil, 2019, p. 215-244

MALLAN, K. Surviving the electronic panopticon: new lessons in Democracy, Surveillance, and Community in Young Adult Fiction. In: ARAYA, D. (ED.). **Smart cities as democratic ecologies**. Houndsmills, Basingstoke, Hampshire; New York: Palgrave Macmillan, 2015, p. 142-158.

MAQUIAVEL, N. **Discursos sobre a Primeira Década de Tito Lívio.** São Paulo: Martins Fontes, 2007.

MARTÍNEZ-BALLESTÉ, A.; PÉREZ-MARTÍNEZ, P. A.; SOLANAS, A. The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible**. IEEE Communications Magazine**, June 2013, pp. 136-141

WOETZEL, J.; REMES, J.; BOLAND, B.; LV, K.; SINHA, S.; STRUBE, G.; MEANS, J.; LAW, J.; CADENA, A.; VON DER TANN, V. **Smart Cities: Digital Solutions For A More Livable Future**. McKinsey Global Institute, 2018. Disponível em: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/Smart%20cities%20Digital%20solutions%20for%20a%20more%20livable%20future/MGI-Smart-Cities-Executive-summary.pdf. Acesso em 08 fev. 2022.

MENEZES, J. B. de; COLAÇO, H. S. Quando a Lei Geral de Proteção de Dados não se aplica? In: FRAZÃO, A.; DONATO OLIVA, M.; TEPEDINO, G. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 2ª edição. São Paulo: Thomson Reuters Brasil, 2020, p. 153-194

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

MOROZOV, E. **Big tech: a ascensão dos dados e a morte da política**. São Paulo: Ubu Editora, 2018.

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

MOURA, F.; DE ABREU E SILVA, J. Smart Cities: Definitions, Evolution of the Concept and Examples of Initiatives. In: LEAL FILHO, W. et al. (Eds.). **Industry, Innovation and Infrastructure**. Encyclopedia of the UN Sustainable Development Goals. Cham: Springer International Publishing, 2019. p. 1–9.

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.

MULHOLLAND, C.; A tutela da privacidade na internet das coisas (IOT). In: SILVA, A. et al.. **Horizonte Presente: tecnologia e a sociedade em debate.** Belo Horizonte: Casa do Direito. Fundação Getúlio Vargas, 2019, p. 485-495

NARAYANAN, S. N.; KHANNA, K.; PANIGRAHI, B. K.; JOSHI, A.; Security in Smart Cyber-Physical Systems: A Case Study on Smart Grids and Smart Cars. In: RAWAT, D.B.; GHAFOOR, K. Z. **Smart cities cybersecurity and privacy**. 1st edition ed. Cambridge, MA: Elsevier, 2018, p. 147-163

NAUTIYAL, L.; MALIK, P.; AGARWAL, A. Cybersecurity System: An essential pillar of Smart Cities. In: MAHMOOD, Z. (ED.). **Smart Cities: Development and Governance Frameworks.** 1st ed. 2018 ed. Cham: Springer International Publishing : Imprint: Springer, 2018, p. 25-50

OAV**. China's Urban Future**. 2019. Disponível em: https:// oav.de/fileadmin/user_upload/Chinas_Urban_Future_web.pdf. Acesso em 10 ago. 2021.

OLIVEIRA, S. R. de. **Sorria, você está sendo filmado! Repensando Direitos na Era do Reconhecimento Facial.** São Paulo: Thomson Reuters Brasil, 2021**.**

PASQUALE, F. **The black box society: the secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015.

QI, R. et al., Blockchain-Powered Internet of Things, E-Governance and E-Democracy. In: **E-democracy for smart cities**. New York, NY: Springer Berlin Heidelberg, 2017, p. 509-520.

QU, Y.; NOSOUHI, M. R.; CUI, L.; YU, S. Privacy Preservation in Smart Cities. In: RAWAT, D.B.; GHAFOOR, K. Z. **Smart cities cybersecurity and privacy**. 1st edition ed. Cambridge, MA: Elsevier, 2018, p. 75-88.

RAMOS, L. F. M.; SILVA, J. M. C. Privacy and Data Protection Concerns Regarding the Use of Blockchains in Smart Cities. Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance. Anais... Em: **ICEGOV2019: 12TH INTERNATIONAL CONFERENCE ON THEORY AND PRACTICE OF ELECTRONIC GOVERNANCE.** Melbourne VIC Australia: ACM, 3 abr. 2019. Disponível em: <https://dl.acm.org/doi/10.1145/3326365.3326410>. Acesso em: 2 abr. 2022

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.

RENNÓ, R.; MILANES, V.; PEÑA, P.; VELASCO, P. Ciudades Inteligentes em Latinoamérica, el ciudadano vigilado. **IV Simpósio Internacional LAVITS – Nuevos Paradigmas de Vigilancia? Miradas desde América Latina**, Buenos Aires, 2016, p. 1-9.

RODOTÀ, S. **A vida na sociedade da vigilância**. Rio de Janeiro: Renovar, 2007.

RODRÍGUEZ, R. E. La privacidad en las ciudades inteligentes. **Revista CES Derecho.** Vol. 10, No. 2, julio –diciembre de 2019, p. 675-695.

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.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Ação Civil Pública nº 1010667-97.2022.8.26.0053.** São Paulo: TJ-SP. Decisão proferida em 22 de março de 2022. Disponível em: https://images.jota.info/wp-content/uploads/2022/03/liminar-metro-reconhecimento-facial.pdf. Acesso em 27 de março de 2022.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: DONEDA, D. et al., (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 21-60.

SENNET, Richard. **Construir e habitar: ética para uma cidade aberta**. 2ª edição. Rio de Janeiro: Record, 2021.

SCHREIBER, A. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: DONEDA, D. et al., (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021, p. 319-338.

SENTILO. **What is Sentilo**. Disponível em: https://www.sentilo.io/wordpress/sentilo-about-product/what-is/. Acesso em 5 de março de 2022.

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

SHAW, J.; GRAHAM, M. Digital information and the right to the city. In: WILLIS, K. S.; AURIGI, A.; ROUTLEDGE (FIRM) (EDS.). **The Routledge companion to smart cities.** New York: Routledge, 2020, p. 61-73.

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.

SOUZA, C. A.; PERRONE, C.; MAGRANI, E. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: In: DONEDA, D. et al.,

(coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 244-270.

SOUZA, C. A.; Capítulo 15 - Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: In: FRAZÃO, A.; DONATO OLIVA, M.; TEPEDINO, G. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 2ª edição. São Paulo: Thomson Reuters Brasil, 2020, p. 413-440.

THEODOROU, S.; SKLAVOS, N. Blockchain-Based Security and Privacy in Smart Cities. In: RAWAT, D.B.; GHAFOOR, K. Z. **Smart cities cybersecurity and privacy**. 1st edition ed. Cambridge, MA: Elsevier, 2018, p. 21-38.

TORRES, F. B.; AZEVEDO, R. **STF e o reconhecimento da existência do direito fundamental à proteção de dados.** JOTA Flash. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/stf-e-o-reconhecimento-da-existencia-do-direito-fundamental-a-protecao-de-dados-05122020?amp=1. Acesso em 23 de março de 2022.

UNCTAD. **Data Protection and Privacy Legislation Worldwide**, 2021. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em 9 de abril de 2022.

UNITED NATIONS. **Sustainable Development – The 17 Goals**, 2015. Disponível em: https://sdgs.un.org/es/goals. Acesso em 12 ago. 2021.

UNITED NATIONS. **HABITAT III Policy Paper 1 – Right to the City and Cities for All.** 2016. Disponível em: <http://habitat3.org/wp-content/uploads/Policy-Paper-1-English.pdf>. Acesso em: 13 ago. 2021.

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 ago. 2021.

VAINZOF, R. Capítulo I - Disposições Preliminares. In: MALDONADO, V. N.; OPICE BLUM, R. (coord.). **Lei Geral de Proteção de Dados Comentada**. 2ª edição. São Paulo: Thomson Reuters Brasil, 2019, p. 19-178

VANDERCRUYSSE, L.; BUTS, C.; DOOMS, M. A typology of Smart City services based on DPIA-costs (D.3.2). **SPECTRE Research Project**, Bruxelas: FWO, 2019. Disponível em: https://spectreproject.be/. Acesso em 25 de março de 2022.

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

WARREN, Samuel D. BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, no. 5, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 20 de março de 2022.

WESTIN, A. F.; SOLOVE, D. J. **Privacy and Freedom**. La Vergne: Ig Publishing, 2018.

WILLEMS, J. et al.. **Do privacy issues matter in citizen participation? An experiment in the context of Smart City apps**. Working Paper, 2017. Disponível em: https://www.researchgate.net/profile/Jurgen_Willems. Acesso em 3 de abril de 2022.

WILLIS, K; AURIGI, A. Introduction. In: In: WILLIS, K. S.; AURIGI, A.; ROUTLEDGE (FIRM) (EDS.). **The Routledge companion to smart cities**. New York: Routledge, 2020, p. 1-12.

WILLIS, K. The death and life of smart cities. In: WILLIS, K. S.; AURIGI, A.; ROUTLEDGE (FIRM) (EDS.). **The Routledge companion to smart cities**. New York: Routledge, 2020, p. 411-428.

WIMMER, M. Interfaces entre Proteção de Dados e Segurança da Informação: um debate sobre a relação entre Direito e Tecnologia. In: DONEDA, D.; MENDES, L. S.; CUEVA, R. V. B. (coords.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018) - A caminho da efetividade: contribuições para a implementação da LGPD.** São Paulo: Thomson Reuters Brasil, 2020, p. 127-144

XAVIER, L. P.; XAVIER, M. P.; SPALER, M. G. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. In: FRAZÃO, A.; DONATO OLIVA, M.; TEPEDINO, G. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2ª edição. São Paulo: Thomson Reuters Brasil, 2020, p. 479-498.

ZUBOFF, Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. In: BRUNO, F. et al. (EDS.). **Tecnopolíticas da vigilância: perspectivas da margem.** 1a edição ed. São Paulo, SP: Boitempo, 2018, p. 15-68.

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).