A PARCERIA PÚBLICO-PRIVADA NA SEGURANÇA DE CIDADES INTELIGENTES E O EQUILÍBRIO ENTRE O INTERESSE PÚBLICO E A PRIVACIDADE INDIVIDUAL

Anderson Araujo Fernandes do Couto[1]
Klemenson Marcolino[2]
Priscila Elise Alves Vasconcelos[3]

INTRODUÇÃO

As cidades inteligentes, ou *smart cities*, se tornaram possíveis devido à revolução digital em curso nas últimas décadas. O novo mundo dos dados e o advento da internet das coisas abriram caminho para diversas soluções tecnológicas para a otimização de processos, economia de recursos e monitoramento de fenômenos naturais e sociais. Nesse contexto, surgiram sensores de presença ligados à rede de iluminação, promovendo a economia energética; sensores climáticos, possibilitando a antecipação do alerta a desastres naturais; câmeras inteligentes capazes de identificar armas de fogo e realizar a identificação facial, reduzindo o índice de crimes, entre diversas outras soluções para problemas da sociedade.

O conceito de cidades inteligentes remonta à década de 80 do século passado. À época, os Estados Unidos da América, avançavam na questão do planejamento urbano, ao passo que novas tecnologias associadas à internet surgiam. No Brasil, os debates sobre políticas urbanas, ensejados pela Constituição Federal de 1988, ganharam força, encontrando a crescente modernização das tecnologias de comunicação e informação (TIC), dando início ao fenômeno das *smart cities*.

Trata-se de um modelo de crescimento urbano que privilegia a utilização de recursos tecnológicos integrados, voltados ao desenvolvimento sustentável, estruturado em onze eixos temáticos, quais sejam: mobilidade e acessibilidade, urbanismo, meio ambiente, educação, saúde, segurança, energia, empreendedorismo, tecnologia e inovação, governança e economia.

Atualmente, o Brasil possui o Programa de Cidades Inteligentes, desenvolvido de acordo com o Decreto nº 9854/19, que instituiu o Plano Nacional de Internet das Coisas. Fruto disso foi editada a Carta Brasileira para Cidades Inteligentes, alinhada à estratégia nacional para desenvolvimento das cidades inteligentes e sustentáveis no Brasil.

No Brasil, a segurança pública das cidades é responsabilidade estadual, por meio das secretarias de segurança pública, efetivada pela atuação das polícias militar e civil. A guarda municipal zela por bens, serviços e instalações, contribuindo assim, para a segurança. Os desafios para a segurança pública são multifacetados e apresentam variações de acordo com a região do país. Há locais onde a violência está mais ligada ao tráfico de drogas, enquanto em outras localidades destaca-se a violência doméstica (SOARES, 2006).

De acordo com Cunha et al (2016), os principais eixos no que tange à segurança urbana, são a privacidade e a prevenção a ilícitos, incluído o uso ilegal de dados sensíveis. Assim, o uso de tecnologias e a implantação de infraestruturas inteligentes contribuem para o

[1]Acadêmico do 6º semestre do Curso de Direito – UFRR (andersoncoutodbv.ac@gmail.com)
[2]Acadêmico do 6º semestre do Curso de Direito – UFRR (klemenson.marcolino@gmail.com)
[3] Professora Adjunta do Instituto de Ciências Jurídicas - CCJ - da Universidade Federal de Roraima. Coordenadora do DINTER UFRR UERJ. Coordenadora do Núcleo de Práticas Jurídicas do ICJ UFRR. Pós-Doutorado em Direito das Cidades pela Universidade do Estado do Rio de Janeiro - UERJ (2020). Doutora em Direito pela Universidade Veiga de Almeida - RJ (2018/2020) (priscila.vasconcelos@ufrr.br)

ISSN: 2525-8508

aumento da segurança e apontam para a criação de centros integrados, como o Centro de Operações do Rio de Janeiro ou de Santos, permitindo resposta rápida e eficiente, integrando diversos agentes de segurança e controle em diversos níveis.

Daí surge a necessidade de discussão do limite entre a privacidade e a segurança, uma vez que cada vez mais dados pessoais são coletados, analisados e compartilhados, como localização, dados bancários, cadastros, interação com as redes sociais, dispositivos de biometria, reconhecimento facial e de voz. Destaca-se ainda o uso crescente de câmeras e drones, associado à grande capacidade de armazenar e processar dados – *big data*.

OBJETIVOS

Nesse ambiente de ampliação da capacidade de aquisição, armazenamento e interpretação de informações particulares, sensíveis e sigilosas, o presente trabalho tem por objetivo apresentar as principais tecnologias empregadas na segurança pública no que tange ao processo de transformação das cidades em cidades inteligentes, ressaltando os benefícios da parceria público-privada. Ademais, serão analisadas as consequências para a privacidade individual e coletiva, abordando as principais legislações em vigor que regulam a proteção de dados no Brasil.

METODOLOGIA

Como metodologia, o trabalho conta com pesquisa bibliográfica na legislação, além de contar com o apoio de trabalhos acadêmicos que abordam a temática da segurança pública no ambiente de cidades inteligentes.

RESULTADOS E DISCUSSÃO

1. Tecnologias usadas na segurança de cidades inteligentes

No âmbito da segurança, é fundamental dispor de redes de dados e voz seguras para que seja feita a gestão e coordenação dos diversos setores envolvidos – polícia militar e civil, guarda municipal, bombeiros e serviço de saúde. Tecnologias simples têm sido implementadas com o objetivo de garantir e acelerar essa comunicação. Cunha et al (2016) cita como exemplo a criação de grupos de mensagens instantâneas, criados por associações de bairros ou por conselhos de segurança. Tal ferramenta possibilita a comunicação imediata de moradores com agentes de segurança, permitindo uma ação muito mais rápida e efetiva no controle e repressão ao crime.

Outra iniciativa que se pode observar é o Botão do Pânico, ou Dispositivo de Segurança Preventivo (DSP), que permite a mulheres vítimas de violência doméstica, ou que se sintam ameaçadas, acionarem um alerta, indicando sua localização às autoridades policiais.

Em Vitória, capital do Espírito Santo, local com os maiores índices de homicídios de mulheres, o dispositivo funciona como gravador de áudio, facilitando a produção de provas contra o agressor e se comunicando em tempo real com a Patrulha Maria da Penha da Guarda Civil Municipal. (CUNHA ET AL, 2016)

Centros de Operações têm se mostrado soluções para grandes cidades, onde a segurança pública é particularmente deficiente e os efetivos policiais são insuficientes. Um monitoramento eficaz interligando diversos sistemas de vigilância e alerta, integrados por meio da internet, permite uma ação coordenada em acidentes de trânsito, desastres naturais,

ISSN: 2525-8508

ações criminosas e até mesmo na busca por desaparecidos. Cunha et al (2016) pontua como positivas as experiências do Rio de Janeiro (RJ) e Santos (SP), que se utilizam da tecnologia para integrar a segurança pública e otimizar a atuação dos diversos órgãos e serviços da cidade.

Nesse sentido, Cunha et al (2016) elenca diversas capacidades características de cidades inteligentes usadas por esses centros de operações: centros de comando e controle para a gestão de emergências; proteção a grupos vulneráveis como vítimas de violência doméstica; videovigilância inteligente (3D) e análise de imagens (gravadas e em tempo real); criptografia e segurança das comunicações; simulação 3D e das potenciais incidências de segurança; verificação e identificação automática de documentos; cibersegurança; sensores de segurança e transporte público; sistemas de localização GPS, entre outras. Destaca-se ainda a instalação em diversas rodovias de câmeras capazes de identificar a placa dos veículos.

2. A parceria público-privada nas cidades inteligentes

Nesse escopo, a iniciativa privada se insere na busca por soluções aos problemas urbanos, dentre eles a criminalidade, não obstante predominar a responsabilidade da Administração Pública na instituição de políticas públicas. Araújo (2019), pontua que as principais tecnologias empregadas na segurança pública consistem no monitoramento urbano, auxiliando o trabalho policial e possibilitando o reconhecimento facial, sistemas de videovigilância, captação biométrica, entre outras. Dessa maneira, a parceria público-privada surge como alternativa ao investimento exclusivamente estatal

A parceria público-privada (PPP) é regida pela Lei Federal n. 11.079/2004, que em seu art. 2º, aduz que "é o contrato administrativo de concessão na modalidade patrocinada ou administrativa". Araújo (2019) aponta que essa modalidade de contrato administrativo apresenta vantagens, uma vez que a iniciativa privada possui maior habilidade no gerenciamento de encargos e riscos além de maior habilidade técnica e capacidade de renovação tecnológica, possibilitando a manutenção dos sistemas, diferentemente da dificuldade que a Administração Pública encontra para impedir o sucateamento de seus sistemas.

Assim, Araújo (2019) defende que o campo da segurança pública pode ser explorado pela iniciativa privada, por meio de PPPs, que são primordiais na implantação de cidades inteligentes, no entanto, o Poder Público, responsável direto pela prestação do serviço de segurança, deve ter atenção especial no tratamento dos dados dos usuários no contexto das cidades inteligentes.

Fruto disso, surge a necessidade de se determinar o alcance e os limites de atuação do poder público e empresas conveniadas no tratamento dos dados pessoais dos cidadãos em um contexto de cidades inteligentes. Araújo (2019) defende que a segurança pode ser entendida como um direito humano, e mais ainda, como um direito humano fundamental. Acrescenta, ainda, que pode ser considerado um direito social, na medida em que visa à proteção de interesses coletivos e difusos, citado no art. 6º da CF/88.

3. A Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/18, regulamenta o uso, proteção e transferência de dados pessoais no Brasil. Essa lei observa os direitos fundamentais da liberdade e privacidade, na livre iniciativa, e no desenvolvimento econômico e tecnológico do país, sendo considerada adequada para proteger a privacidade e o uso de dados no país.

ISSN: 2525-8508

No entanto, o art. 4º, inc. III da LGPD, afasta sua aplicabilidade quando o tratamento de dados se dá exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão a infrações penais, com fulcro no princípio da supremacia do interesse público sobre o privado. Essa norma possibilita que órgãos de segurança pública não sejam submetidos às normas desse diploma legal.

Tal prerrogativa pode causar prejuízo à proteção da privacidade e ao exercício da liberdade de expressão, especialmente durante governos autoritários, nos quais pode haver o uso da força estatal para coibir e cercear opositores.

É importante ressaltar que a LGPD, fala expressamente em atividades de investigação e repressão, deixando em aberto quanto à prevenção. Devido à infraestrutura das cidades inteligentes, no que tange à segurança, fazer uso de tecnologias também preventivas, Araujo (2016) entende que, ainda que o art. 4º, III do aludido diploma exclua o Poder Público de se submeter a seus limites quanto atuar no campo da segurança pública, existem limites a serem observados.

Em uma ponderação entre o princípio da supremacia do interesse público sobre o privado e os princípios da LGPD, deve-se observar a proporcionalidade, de maneira que quanto maior o grau de prejuízo do princípio minorado, maior deve ser a importância do cumprimento do princípio que prevalece.

A LGPD, em seu art. 4º, § 2º, disciplina que "É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo".

Complementarmente, § 4º citado, prescreve que "Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. Assim, nas PPP, o setor privado age no lugar do Poder Público, para suprir suas deficiências de infraestrutura e prestação de serviços, situação na qual a Administração Pública deve exercer a tutela administrativa.

Salienta-se, que o direito à privacidade, previsto no art. 5º, X, da CF/88, não pode ser mitigado pelo interesse público, mas ambos devem coexistir em harmonia, após devido sopesamento. Dessa maneira, a Administração Pública, deve observar a proporcionalidade e razoabilidade no uso de dados, além dos demais princípios constitucionais e da administração, não eximindo da responsabilidade no uso inadequado de dados particulares, sob pena de incorrer em ilegalidade seja por desvio ou excesso de poder. (ARAÚJO, 2019)

CONSIDERAÇÕES

Do estudo realizado, conclui-se que as parcerias público-privadas apresentam benefícios para a estruturação de cidades inteligentes, inclusive no que se refere à segurança pública, pois possui maior habilidade no gerenciamento de encargos e riscos além de maior habilidade técnica e capacidade de renovação tecnológica, possibilitando a manutenção dos sistemas, diferentemente da dificuldade que a Administração Pública encontra para impedir o sucateamento de seus sistemas.

A principal legislação que regra a proteção de dados é a Lei nº 13.709/2018, porém sua aplicabilidade é afastada quando o tratamento de dados se dá exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão a infrações penais, tornando necessária a análise de diversos princípios para

ISSN: 2525-8508

determinar os limites da supremacia do interesse público - no caso a segurança - frente a privacidade individual. Nessa análise, nenhum princípio pode ser desconsiderado, mas sopesando de acordo com o caso concreto, levando-se em consideração, principalmente, os princípios da razoabilidade e proporcionalidade.

REFERÊNCIAS

ARAÚJO, Douglas da Silva. **Smart cities, segurança pública e proteção de dados:** uma análise do uso de dados pessoais pelo poder público. 2019. Dissertação de Mestrado. Programa de Pós-Graduação em Direito. UFRN. Natal, 2019. Disponível em: Smartcitiessegurança_Araújo_2019.pdf (ufrn.br). Acesso em: 03 out 22

BRASIL. **Carta Brasileira para Cidades Inteligentes**. Disponível em: https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-urbano/carta-brasileira-para-cidades-inteligentes/20201208_carta-brasileira-para-cidades-inteligentes_final.pdf. Acesso em 03 out 22.

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

BRASIL. Decreto n. 9.854, de 25 de junho de 2019. **Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.** Brasília, DF. 2019.

BRASIL. Lei nº 11.079 de 30 de dezembro de 2004. **Institui normas gerais para licitação e contratação de parceria público-privada no âmbito da administração pública**. Brasília, DF. 2018.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF. 2018.

BRIA, Francesca; MOROZOV, Evgeny. **A cidade inteligente:** tecnologias urbanas e democracia. Ubu Editora, 2020.

CHIUSOLI, Cláudio Luiz; REZENDE, Denis Alcides. Indicadores para uma cidade inteligente e estratégica. **Revista Políticas Públicas & Cidades-2359-1552**, v. 8, n. 1, 2019. Disponível em: https://www.researchgate.net/publication/334231284_Indicadores_para_uma_cidade_inteligente_e_estrategica. Acesso em 03 out 22.

CUNHA, Maria Alexandra. et al. **Smart cities**: transformação digital de cidades. 1ª Ed. São Paulo: FGV, 1ª Ed. 2016. 164p. Disponível em: http://hdl.handle.net/10438/18386. Acesso em 03 out 22

SOARES, Luiz Eduardo. **Segurança Pública**: presente e futuro. Estudos Avançados, São Paulo, v. 20, n. 56, p. 91-106, abr. 2006. Disponível em: SciELO - Brasil - Segurança pública: presente e futuro Segurança pública: presente e futuro. Acesso em: 03 de outubro de 2022.

ISSN: 2525-8508

VIANA, Ana Cristina Aguilar; BERTOTTI, Bárbara Mendonça. Smart cities e o outro lado da moeda: a sociedade de vigilância: Smart cities and the other side of the coin: the surveillance society. **International Journal of Digital Law**, v. 2, n. 1, p. 45-46, 2021. Disponível em: Smart cities e o outro lado da moeda: a sociedade de vigilância | Sumários.org (sumarios.org). Acesso em 03 out 22

ISSN: 2525-8508