REVISTA

DOI: 10.56119/rcabdc.v7.104

V.7, 2026, ISSN 2318-602X
p.101-123
https://abdc.emnuvens.com.br/abdc

DESTAQUE

Desafios para a proteção dos dados pessoais e privacidade em cidades inteligentes: análise da proposta de reforma do Código Civil brasileiro[1]

Challenges for the protection of personal data and privacy in smart cities: analysis of the proposed reform of the brazilian Civil Code

Isabella Souza Rainho de Oliveira Poli
Orcid: 0009-0006-4348-2128

Paloma Fernandes Lins Barca
Orcid: 0009-0009-1596-3225

Resumo

O presente trabalho tem como objetivo analisar as cidades inteligentes que utilizam inteligência artificial no tratamento de dados pessoais, investigando os desafios relacionados à privacidade e proteção de dado dos cidadãos nesse contexto. Para tanto, foi realizada uma pesquisa através dos métodos de abordagem dedutivo e analítico, utilizando levantamento de documentação direta, além da análise e compreensão da legislação e doutrina. Como resultado, foi possível

[1]Artigo apresentado no XII Congresso Intercontinental de Direito Civil, realizado em Coimbra, Portugal nos dias 14 e 15 de novembro de 2024.

CC BY

concluir que a implementação de ferramentas baseadas em inteligência artificial deve observar as disposições da LGPD, com o propósito de assegurar a proteção da privacidade e dos dados pessoais dos cidadãos das cidades inteligentes.

Palavras-chave: Cidades inteligentes; Proteção de dados; Inteligência Artificial; Privacidade.

Abstract

This study aims to analyze smart cities that use artificial intelligence in the processing of personal data, investigating the challenges related to citizens' privacy and data protection in this context. To this end, the research was conducted using deductive and analytical approaches, with direct documentation review, in addition to the analysis and interpretation of legislation and legal doctrine. The results indicate that the implementation of artificial intelligence-based tools must comply with the provisions of the LGPD in order to ensure the protection of citizens' privacy and personal data in smart cities.

Keywords: Smart cities; Data protection; Artificial Intelligence; Privacy.

Introdução

Nos últimos anos, o avanço das tecnologias de inteligência artificial tem impulsionado o desenvolvimento das chamadas cidades inteligentes, prometendo melhorias significativas na qualidade de vida dos cidadãos.

Ocorre, todavia, que os avanços tecnológicos trazem consigo questões cruciais sobre a proteção de dados pessoais dos cidadãos e, nesse sentido, o presente artigo propõe uma análise do impacto da legislação brasileira, especialmente a Lei Geral de Proteção de Dados (LGPD), na implementação de tecnologias de inteligência artificial que tratam dados pessoais nos sistemas implantados nas cidades inteligentes. Propõe-se a referida pesquisa por meio da observação da legislação vigente e doutrina, utilizando levantamento de documentação direta, análise e compreensão da legislação e doutrina, tendo como objetivo a identificação dos principais desafios associados à privacidade e à proteção de dados dos cidadãos no contexto das tecnologias de inteligência artificial nas cidades inteligentes.

1 Metodologia

Inicialmente, é necessário abordar brevemente o conceito de metodologia. Para Richardson (1.999, p.22), "são regras estabelecidas para o método científico, por exemplo: a necessidade de observar, a necessidade de formular hipóteses, a elaboração de instrumentos, etc." Em pesquisa, significa a escolha de procedimentos sistemáticos para a descrição e explicação dos fenômenos. Dessa forma, a pesquisa deve ser planejada e executada em conformidade com as normas estabelecidas para cada método de investigação.

Vale mencionar que as características dos métodos científicos são aplicáveis a qualquer tipo de ciência, desde as biológicas até as sociais, pois estão atreladas ao processo de conhecimento. Para Richardson (1.999, p.30), o que muda é a aplicação das regras e instrumentos. Assim, para estudar fenômenos sociais, utilizamos instrumentos qualitativos, não quantitativos.

Neste estudo, recorre-se aos métodos hipotético-dedutivo, através de pesquisa bibliográfica e documental. Ao abordar a legislação aplicável, parte-se da dedução para explicitá-la em face da sociedade brasileira. Em seguida, realiza-se um estudo fragmentado dos tópicos de trabalho, extraídos tanto da doutrina indicada na bibliografia, visando apreender os conceitos aplicáveis e promover o embate teórico entre posições doutrinárias, em face dos problemas a serem tratados (revisão bibliográfica).

Além disso, considera-se o materialismo para compor e integrar a discussão à realidade social, levando em conta o contexto de reprodução social e cultural que orienta a contemporaneidade, buscando fundamentos sólidos.

Por fim, o caminho percorrido conduz à perspectiva da pesquisadora, de modo orientado, a investigar a influência da imersão social no mundo digital em relação à privacidade e proteção de dados, considerando a aplicabilidade das normas.

O presente projeto de pesquisa reveste-se de atualidade, interdisciplinaridade, pertinência, caráter científico, modo de integração entre teoria e prática, e relevância social e jurídica.

2 Cidades Inteligentes

De acordo com o Relatório Mundial das Cidades, publicado pelo ONU-Habitat em 2022, as áreas urbanas têm a projeção de abrigar 68% da população mundial até 2050 (ONU-HABITAT, 2022). No Brasil, esse percentual já alcança a proporção de 61% conforme dados do IBGE (IBGE, 2022).

O acelerado crescimento populacional nas áreas urbanas impõe desafios significativos para os governos e é neste contexto que se revela imprescindível as pesquisas acerca do tema.

O conceito de cidades inteligentes, ou *smart cities*, refere-se a uma cidade com "processos informatizados sensíveis ao contexto, lidando com um gigantesco volume de dados (Big Data), redes em nuvens e comunicação autônoma entre diversos objetos" (LEMOS, 2013, p.48). Trata-se de uma cidade que processa um grande número de informações que servem como base para integração de infraestruturas físicas, sociais, ambientais e digitais, com o objetivo de promover uma gestão mais eficiente e sustentável dos centros urbanos.

Nas cidades do futuro, assim também denominadas, as tecnologias da informação e comunicação (TIC) desempenham um papel essencial, uma vez que podem fornecer os meios para o monitoramento e a gestão dos serviços e recursos das infraestruturas urbanas. Além disso, as TIC oferecem a possibilidade de aproximar o poder público dos cidadãos através de serviços eletrônicos disponibilizados na internet (WEISS; BERNARDES; CONSONI**.**, 2017, p.3), criando um sistema interconectado, um conjunto orgânico e sistêmico (RECH, 2020, p.106).

Para tornar esse cenário factível, é essencial que essas cidades disponibilizem ferramentas aptas a analisar os dados coletados para gestores e cidadãos, apoiar à garantia de privacidade e transparência de dados e melhorar serviços ofertados aos cidadãos. Em todas essas categorias, o uso da Inteligência Artificial (IA) tem permitido aprimorar os processos de tomada de decisão em diversas situações complexas (BERNARDINI; BARCELLOS; CRUZ, 2020, p.29).

Importa mencionar que "a inteligência artificial é um ramo da ciência da computação que se concentra no desenvolvimento de algoritmos e sistemas capazes de realizar tarefas que normalmente exigem inteligência humana" (TELLES, 2023, sem paginação).

3 Evolução social e Perspectivas sobre aplicações da IA em cidades inteligentes

A sociedade está em constante evolução, adaptando-se ao meio em que vive, com os anseios da população diretamente influenciados pela direção da economia. Inicialmente, predominava uma sociedade agrícola, onde a fonte de riqueza provinha da terra e a economia era impulsionada pelo escambo de produtos agrícolas. Posteriormente, houve uma transição para uma sociedade industrial, na qual as máquinas a vapor e a eletricidade assumiram um papel central na produção.

Com o término da Segunda Guerra Mundial, evoluímos para uma sociedade pós-industrial, caracterizada pelos serviços oferecidos, como bancários, securitários, educacionais, médicos, jurídicos, entre outros. Atualmente, o elemento central do desenvolvimento econômico é a informação, resultado da evolução tecnológica. Em 2008, as maiores empresas mundiais eram do setor petrolífero, enquanto, em 2018, as empresas de tecnologia dominaram economicamente o mundo, levando ao surgimento do jargão "os dados são o novo petróleo mundial".

O avanço tecnológico, aliado ao aumento da capacidade de processamento, reduziu o tempo e o espaço no mundo, conectando as pessoas e gerando uma quantidade massiva de dados, a economia mundial passou a ser direcionada através de dados, estabelecendo uma cultura denominada "*data-driven economy*", marcando uma transição causada pelo surgimento de novas tecnologias de extração e análise de dados (FRAZÃO, 2020).

Este modelo de cultura tornou a extração de dados pessoais uma atividade econômica baseada na vigilância sobre a vida dos indivíduos, registrando os hábitos, deslo-

camentos, padrões de consumo e tudo o que for possível extrair, armazenar e analisar. A este sistema econômico, Zuboff deu o nome de capitalismo de vigilância, e o classificou como 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).

Conforme cita Bruno Bioni (2019, p.30), a sociedade, está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia e, neste cenário evolutivo, os mecanismos de processamento passaram a ser capazes de processar e transmitir informações em velocidades inimagináveis.

Destarte, o espaço urbano, com a possibilidade de introdução das novas tecnologias, torna-se um terreno a ser desbravado pela economia movida a dados. É fato que, diante do inchaço dos centros urbanos decorrentes da migração da população, a aplicação destes mecanismos pode ser acompanhada de ganhos de qualidade de vida e a 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, contudo, a sociedade precisa estar cada vez mais consciente de que o excesso de vigilância pode ser problemático.

Para que sejam atingidos os benefícios propostos pelas cidades inteligentes que visam a união do uso das tecnologias como processamento de dados e inteligência artificial, permitindo, por exemplo, melhoria na prestação dos serviços públicos e dos negócios, bem como o acesso pela população com melhor atendimento das necessidades desta, proteções jurídicas e decisões políticas são necessárias (PRADO FILHO, 2020, p. RB-3.1).

A inteligência artificial desempenha um papel crucial no futuro das cidades, especialmente por sua capacidade de processar grandes volumes de dados em tempo real, podendo contribuir para melhorias e desenvolvimento dos centros urbanos (TELLES, 2023, sem paginação).

A exemplo de aplicações de IA que geram benefícios em cidades ao redor do mundo, observa-se o sistema de "reconhecimento facial utilizado pela polícia de Londres é baseado em tecnologia de inteligência artificial, que permite analisar imagens capturadas por câmeras de segurança instaladas em locais públicos. As imagens são comparadas com bancos de dados de suspeitos procurados, incluindo pessoas procuradas por crimes graves, como terrorismo e assassinato. Quando uma correspondência é encontrada, os oficiais são alertados para verificar a identidade da pessoa e tomar medidas apropriadas" (TELLES, 2023, sem paginação).

Outro exemplo ocorre em Singapura, utilizam a tecnologia de gerenciamento de tráfego inteligente, o "sistema usa uma combinação de câmeras e sensores para monitorar o tráfego em toda a cidade, permitindo que os algoritmos de IA otimizem os tempos de sinalização dos semáforos para reduzir o congestionamento e melhorar a fluidez do tráfego" (TELLES, 2023, sem paginação).

Por oportuno, cumpre mencionar os ensinamentos de Ana Frazão (2019, p. 109) no sentido de que hoje a privacidade não apenas dispõe acerca da intimidade e ao direito de ser deixado só, mas também abrange outros direitos do indivíduo, como o direito de controle sobre as informações pessoais, autodeterminação informativa, liberdade, privacidade, igualdade, acesso e não discriminação.

Por sua vez, as normas e legislações que trazem diretrizes para a construção de uma sociedade ética não evoluíram na mesma velocidade que a tecnologia, o que vem ocasionando riscos ao controle social neste novo universo digital, especialmente no que tange à garantia dos indivíduos de sua privacidade e da proteção de seus dados pessoais, informações essas que são consideradas uma extensão da personalidade.

Este fenômeno de imersão social no mundo digital, onde os algoritmos passam a orquestrar as vidas das pessoas, impõe a necessidade de estabelecer normas capazes de conter o efeito corrosivo das relações humanas, garantindo o livre exercício da personalidade. E, nesse sentido, o Brasil tem buscado regulamentar essas questões

através de legislações como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), a garantia da Proteção de Dados como um direito fundamental, além de projetos de regulamentação da inteligência artificial e propostas de alteração do Código Civil.

4 Da proteção de dados pessoais e privacidade

Para a implementação de soluções de tecnologia de inteligência artificial que realizam o tratamento de dados pessoais nas cidades inteligentes, é importante assegurar a privacidade e a proteção das informações dos cidadãos. Revela-se necessária, portanto, a análise da temática de proteção de dados pessoais das ferramentas de tecnologia implantadas nas cidades inteligentes que utilizam de inteligência artificial e tratam dados pessoais dos cidadãos.

Nesse contexto, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e desenvolvimento pessoal das pessoas físicas, o Brasil regulamentou, por meio da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal nº 13.709/2018), o tratamento dos dados pessoais, atribuindo regras para os agentes de tratamento, sob pena de a inobservância da referida lei implicar às instituições públicas ou privadas penalidades legais.

Importante esclarecer que a legislação brasileira seguiu, na verdade, uma tendencia mundial de proteção à privacidade e proteção de dados, tendo sido especialmente influenciada pelo Regulamento Geral de Proteção de Dados da União Europeia, promulgado em 2016, o qual foi antecedido, inclusive, por estudos e publicações como o *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* em 1980 pela OCDE (Organização para a Cooperação e o Desenvolvimento Econômico) e pelo Conselho da Europa, pela aprovação do *Explanatory Report on the Convention for Protection of Individual with Regard to Automatic Processing of Personal Data* em 1981, pela Diretiva de Proteção de Dados (Diretiva 95/46/EC de 1995) e Convenção que vinculou os Estados da União Europeia a internalizarem regramento acerca da

privacidade e proteção de Dados (Convenção 108 do Conselho da Europa, de 1981) (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 17/19).

Ainda, importante lembrar que, com o propósito de assegurar a proteção dos dados pessoais como um direito fundamental, a Emenda Constitucional n. 115/2022 incluiu o inciso LXXIX no art. 5 da Constituição Federal Brasileira, tendo a disposição estabelecido que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Com a proteção de dados "é concedido ao privado um poder de controle direto e contínuo sobre os coletores de informações, independentemente da existência real de uma violação. Muda assim a técnica de proteção da privacidade e a atenção se desloca para o bom funcionamento das regras sobre a circulação das informações" (RODOTÀ, 2008, p. 60).

E, para que haja o tratamento das informações pessoais por sistemas de inteligência artificial nas cidades inteligentes, se revela essencial assegurar transparência aos cidadãos como titulares dos dados, tanto aqueles que têm suas informações tratadas de forma direta ou indiretamente, especialmente porque o mencionado tratamento pode influenciar diretamente ao livre desenvolvimento do pensamento e desenvolvimento da personalidade dos cidadãos.

Nesse sentido, Rodotà sugere uma interligação entre a esfera política e privada do indivíduo, em que as condições gerais do funcionamento do sistema político influenciam no grau de proteção que o indivíduo possui em sua esfera privada e, por sua vez, "as regras de circulação das informações estão destinadas a incidir sobre a distribuição de poder na sociedade", se revelando, deste modo, imperiosa a proteção da esfera privada do cidadão (RODOTÀ, 2008, 45).

Ana Frazão (2019, p. 102) também reflete que atualmente a análise da privacidade não é mais devida sob a noção tradicional de intimidade e direito de ser deixado só, ponderando, por outro lado, a necessária abordagem contextualizada e que abarque os desafios ensejados pela economia movida a dados e vigilância.

Aliás, considerando as novas formas de relação humana, é inequívoco que a proteção de dados foi reinventada, pois além de se tratar de um direito fundamental, também consiste em uma ferramenta necessária ao livre desenvolvimento da personalidade, podendo ser vista, inclusive, como um conjunto de direitos que configuram a cidadania no novo milênio (RODOTÀ, 2008, p. 15).

Com efeito, conforme bem pontua Rodotà (2008, p. 28):

> É bem evidente, de fato, que o enorme aumento da quantidade de informações pessoais coletadas por instituições públicas e privadas visa sobretudo a dois objetivos: a aquisição dos elementos necessários à preparação e gestão de programas de intervenção social, por parte dos poderes públicos, e o desenvolvimento de estratégias empresariais privadas; e o controle da conformidade dos cidadãos à gestão política dominante ou aos comportamentos prevalecentes.

Como bem ponderou Rodotà "É necessário realizar balanceamentos mais complexos entre os interesses em jogo, para assegurar a coexistência da garantia dos direitos individuais com a abertura da sociedade." (RODOTÀ, 2008, p. 48).

Importante esclarecer ainda que, nos termos do artigo 44 da LGPD, o tratamento será irregular quando não observar a legislação ou não fornecer a segurança que o titular espera, considerando a forma que o tratamento é realizado, o resultado e riscos que se esperam do tratamento e as técnicas de tratamento disponíveis. E, sendo a operação considerada irregular, consistirá em uma violação ou incidente de segurança.

Para a LGPD, tratamento de dado pessoal é qualquer operação realizada com o dado pessoal ou dado pessoal sensível, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração da informação relacionada a uma pessoa natural identificada ou identificável, consoante determinado no art. 5º, inciso X.

Por sua vez, importante esclarecer que, nos termos do art. 4º, inciso III da LGPD, a legislação não se aplica quando a operação tem fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação penal.

Em que pese haver as excepcionalidades citadas para não aplicação à LGPD, por outro lado, a regra para o Poder Público é a observância a referida legislação e o deve ser em razão de os dados consistirem em um importante recurso para que sejam desenvolvidas políticas públicas e administração mais eficiente e assertiva e, desta forma ocorre com a implementação de tecnologias com uso de inteligência artificial e análise de dados pessoais nas cidades inteligentes.

As cautelas necessárias para o tratamento dos dados pessoais públicos se revelam imprescindíveis para além da proteção dos direitos dos titulares, pois promove a tutela da cidadania e das instituições democráticas, razão pela qual, inclusive, a LGPD se trata de uma norma restritiva da ação estatal, visto que trouxe regramentos para as operações realizadas com dados pessoais, inclusive o dever de observância aos princípios da aludida legislação (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 211).

E, nesse sentido, vale ressaltar que o art. 6º da LGPD discorre acerca dos princípios que devem ser observados como diretrizes essenciais para qualquer tratamento de informações, quais sejam: i) finalidade; ii) adequação; iii) necessidade; iv) livre acesso; v) qualidade dos dados; vi) transparência; vii) segurança; viii) prevenção; ix) não discriminação e x) responsabilização. Assim, tais princípios devem ser observados para todo e qualquer tratamento de dados pessoais inclusive havidos pelo Poder Público, igualmente no tocante às ferramentas que faça uso de inteligência artificial implementada nas cidades inteligentes.

Ainda, vale ressaltar o papel da Autoridade Nacional de Proteção de Dados Brasileira – ANPD que, nos termos do art. 5º, inciso XIX da LGPD, é a autarquia brasileira responsável pela implementação fiscalização e cumprimento da referida legislação. Cumpre esclarecer, ainda que o art. 55-J da LGPD discorre acerca das competências da referida Autoridade, dentre as quais se destacam a elaboração de estudos sobre as práticas nacionais de proteção de dados e articulação com autoridades reguladoras públicas para exercer competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação.

Em razão disso, dentre os documentos publicados pela ANPD, destaca-se o "Cidades inteligentes", o qual especificamente analisa a temática das cidades inteligentes com ênfase na proteção de dados (BRASIL, 2024).

E, na referida pesquisa foi analisada a vultosa coleta de dados pessoais dos cidadãos e destacada a preocupação social e governamental quanto aos riscos de: i) vigilância e controle do cidadão, pois os dados coletados podem gerar relatórios detalhados sobre os titulares das informações, fato que implicaria em uma assimetria de informações e poder; ii) uso comercial dos dados, tendo em vista que empresas de fornecedores possuem acesso à informações quando do oferecimento do serviço ao poder público; iii)vazamento de dados, uma vez que o aumento da quantidade de informações cria exposições de dados ou quebra de privacidades, bem como a vulnerabilidade para ciberataques pelo uso de dispositivos conectados, circunstancias que poderiam permitir criminosos utilizarem de tais informações para cometer atos ilíticos; iv) usos não esperados pelo desvio de finalidade; v) compartilhamento de maneira inadequada entre órgãos públicos e para com o setor privado; vi) discriminação e aspectos éticos em razão da possibilidade de algoritmos poderem reforçar vieses sociais, discriminando indivíduos, prejudicando vulneráveis e; vii) perda da qualidade do dado por informações enviesados ou imprecisos (BRASIL, 2024, p. 15/16).

Somada a proteção como direito fundamental e as precisas disposições previstas na LGPD, em razão da sociedade contemporânea, novas formas de relacionamentos sociais por meio das plataformas digitais, bem como das discussões acerca do direito civil digital, uma Comissão de Juristas destinados para tal finalidade, desenvolveu um trabalho de proposta de revisão e atualização do Código Civil Brasileiro, pelo que, dentre outras disposições e proposições, no presente artigo concentra naquelas que são relacionadas à proteção de dados e dos avanços da inteligência artificial que destacaram a importância da responsabilidade por parte dos desenvolvedores e operadores desses sistemas, uma vez que estão especialmente relacionados ao desenvolvimento do presente artigo, tendo em vista a relação entre os sistemas das

cidades inteligentes com uso de inteligência artificial e tratamento de dados pessoais e as implicações de eventuais exposições dos titulares à incidentes de segurança ou de tratamento para finalidades distintas das que tais informações foram coletadas, podendo, inclusive, como visto, influenciar ao livre desenvolvimento da personalidade e integridade mental do titular.

Desse modo, a disciplina do Direito civil digital proposta pela mencionada Comissão busca fortalecer o exercício da autonomia privada, preservar a dignidade humana, segurança do patrimônio e estabelecer critérios para a definição da legalidade e regularidade dos atos e atividades desenvolvidas no ambiente digital (BRASIL, 2023, p. 239).

Dentre outros fundamentos da disciplina do direito civil digital, a comissão estabelece: I. o respeito à privacidade, proteção de dados pessoais e patrimoniais, autodeterminação informativa; III. inviolabilidade da intimidade, honra, vida privada, imagem da pessoa; IV. Desenvolvimento e inovação econômicos, científicos e tecnológicos, assegurando a integridade e privacidade mental, liberdade cognitiva, o acesso justo, a proteção contra práticas discriminatórias e a transparência algorítmica; VII. o efetivo respeito aos direitos humanos, livre desenvolvimento da personalidade e dignidade das pessoas e o exercício da cidadania pelas pessoas naturais (BRASIL, 2023, p. 239).

A proposta ainda discorre como um dos parâmetros fundamentais para a interpretação das atividades civis a garantia da segurança no ambiente digital pelos sistemas de proteção de dados e que sejam capazes de proteger os usuários contra ações que possam limitar a capacidade de julgamento, ainda que temporária (BRASIL, 2023, p. 238). Além disso, a proposta preconiza, dentre os direitos às pessoas no ambiente digital, a proteção dos dados e informações pessoais, garantia dos direitos da personalidade em todas as expressões, como a dignidade, honra, privacidade e livre desenvolvimento (BRASIL, 2023, p. 239).

Ainda, a proposta traz uma série de proteções aos neurodireitos, os quais consideram proteções que buscam preservar a privacidade mental, identidade pessoal, livre arbítrio, acesso justo à ampliação e melhoria cerebral, integridade mental e proteção

contra vieses a partir de utilização de neurotecnologias, e reconhece, além disso, a identidade digital como meio de identificação oficial nos ambientes digital (BRASIL, 2023, p. 242), direitos esses que também devem ser protegidos na hipótese de implantação de um sistema de inteligência artificial com tratamento de dados pessoais nas cidades inteligentes.

Além disso, a mencionada proposta preconiza resguardar os direitos fundamentais, garantindo a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana e do desenvolvimento científico e tecnológico, de modo que determinou para o desenvolvimento de sistemas de inteligência artificial que seja resguardado aos cidadãos, em síntese: i) a não discriminação em relação ao uso de dados, processos e decisões; ii) requisito de transparência, auditabilidade, explicabilidade, rastreabilidade, supervisão humana e governança; iii) acessibilidade, usabilidade, confiabilidade e; iv) necessidade de atribuição de responsabilidades pelos atos da inteligência artificial a uma pessoa natural ou jurídica, sendo requisito, ainda, o monitoramento quando houver desenvolvimento e uso de inteligência artificial ou robótica relacionado a direitos fundamentais (BRASIL, 2023, p. 251).

Na proposta de reforma, é garantido às pessoas naturais que venham a sofrer danos devido à operação de sistemas de inteligência artificial, o direito de serem informadas sobre suas interações com o sistema, seu modelo de funcionamento e os critérios utilizados para decisões automatizadas que possam impactar seus direitos ou interesses econômicos (BRASIL, 2023, p. 251).

5 O tratamento de dados pessoais pelo Poder Público nos termos da LGPD

Para a análise da implantação de sistemas de inteligência artificial que façam uso de tratamento de dados pessoais em cidades inteligentes, é necessário também a análise do regramento feito pela LGPD, a qual trouxe um cômpito específico

para o tratamento de Dados Pessoais pelo Poder Público, isto é, o Capítulo IV e, no referido capítulo destaca-se especialmente dois artigos, quais sejam, 25 e 26.

No art. 25, a referida legislação regulamenta o uso compartilhados de informações pessoais pelo Poder Público, bem como a necessidade de tais dados serem estruturados e mantidos em formato interoperável para o uso compartilhado com o propósito de execução de políticas públicas, prestação de serviços públicos, descentralização da atividade pública e disseminação e acesso das informações pelo público.

Por sua vez, no art. 26, a LGPD determina a necessidade de observância aos princípios anteriormente explanados, previstos no art. 6º, e de atendimento às finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas. Note-se, portanto, que para haver o compartilhamento de dados entre a Administração Pública é necessário que tal tratamento seja de forma clara, de acordo com as hipóteses de tratamento e atenda os direitos dos titulares (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 228).

D'outro lado, vale ainda mencionar que a LGPD disciplina que o compartilhamento de dados do Poder Público para com pessoas jurídicas de direito privado é excepcionalmente permitido quando nas hipóteses específicas e, nas permissões havidas, deve observar requisitos e procedimento específico disposto no art. 26 e seguintes, sendo necessário, ainda, a informação da existência do compartilhamento para com a Autoridade Nacional de Proteção de Dados, informação essa que, de acordo com o parágrafo único do art. 27, depende de regulamentação e possibilidade de a referida autoridade estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados.

E, ainda, nos termos do art. 24 da LGPD, as sociedades de economia mista ou empresas públicas que atuem em regime de concorrência sujeitam-se às regras das entidades privadas e, por sua vez, se estiverem operacionalizando políticas públicas e no âmbito da execução destas, submetem-se às regras de tratamento de dados dispensadas ao Poder Público.

Assim, para a implantação de ferramentas de tecnologia que realizam o tratamento de dados pessoais com uso de inteligência artificial, caso consista em finalidade divergente, se revela necessária a adequação para que não consista em um tratamento em desacordo à legislação, podendo, nessa hipótese, inclusive, utilizar-se do consentimento do titular. Além disso, caso a ferramenta não seja do próprio Poder Público, mas sim gerenciada por empresa privada, há de haver a avaliação de como deverá ser promovido o compartilhamento, sua possibilidade para o caso específico e, se haverá a necessidade de informar a Autoridade Nacional de Proteção de Dados, conforme explanado.

É importante lembrar que a complexidade do Poder Público e da estrutura organizacional e das políticas e ações implica na necessidade de desempenho de ações conjuntas por vários órgãos da mesma pessoa jurídica de direito público ou de mais de uma pessoa jurídica de direito público, circunstância que implica em distinta relevância acerca do compartilhamento de dados pelo poder público (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 226).

Além disso, é necessário que as ferramentas implementadas nas cidades inteligentes que realizem quaisquer tratamentos de dados pessoais assegurem a proteção à Democracia, pois "há relação umbilical entre o autoritarismo e vigilância, não só porque governos autoritários se utilizam reiteradamente de técnicas de vigilância, mas também porque o excesso de vigilância é um incentivo para o autoritarismo, ao propiciar muita concentração de poder" (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 8).

E, nesse aspecto, as ferramentas de tecnologia com uso de inteligência artificial nas cidades inteligentes que propõem a análise e tomada de decisões com base nos dados pessoais dos cidadãos devem observar às disposições e regulamentos para proteção de dados, inclusive, adotando boas práticas para a governança das informações e proteção dos titulares das informações.

6 A proteção de dados em aplicações com uso de inteligência artificial em cidades inteligentes: desafios e boas práticas

Como visto, é necessário que haja a integração dos controles individuais e coletivos, de modo que a proteção de dados não pode se limitar a aspectos isolados, ainda que de extrema relevância, mas deve adotar estratégias integradas que assegurem e regulem o controle da circulação de informações de maneira abrangente, especialmente porque a análise de informações se trata de meios imprescindíveis para o enfrentamento de situações de emergência em matérias de ordem pública (RODOTÀ, 2008, p. 50 e 51).

E, nesse sentido, afirmações de que a violação da privacidade deve ser aceita ou considerada como o preço a ser pago para que seja permitido o acesso a serviços mais eficientes devem ser vistos com a devida cautela, devendo, haja vista que inexiste evidências de que tais benefícios não poderiam ser acessados por tecnologias que respeitem a privacidade e dados pessoais (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 7).

E é importante que haja sistematicidade na interpretação da LGPD, uma vez que "o tratamento de dados pessoais pelo Estado se dê não apenas de modo a legitimamente promover a sua eficiência e modernização, mas também de forma a resguardar direitos individuais e coletivos associados à privacidade e à proteção de dados pessoais" (WIMMER, 2019, p. 133).

Deste modo, também é necessário que tais sistemas das cidades inteligentes assegure os direitos dos titulares, os quais devem ser analisados juntamente com a aplicação das hipóteses legais permissivas de tratamento, e estão previstos no art. 18 da LGPD, quais sejam: i) confirmação da existência de tratamento; ii) acesso aos dados; iii) correção dos dados incompletos, inexatos ou desatualizados; iv) anonimização, bloqueio eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; v) portabilidade dos dados a outro fornecedor de

serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; vi) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD; vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dado; viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e ix) revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

Além dos direitos dos cidadãos, na condição de titulares dos dados, para que os sistemas das cidades inteligentes estejam adequados à LGPD também é indispensável que adote boas práticas e medidas de segurança, as quais estão previstas no art. 46 e seguintes da LGPD. E, nesse sentido, o programa de governança em privacidade, a ser seguido por empresas e órgãos, deve ser fundamentado na garantia dos direitos do titular, resguardando o livre acesso aos dados, garantia da exatidão, transparência, segurança, prevenção, responsabilização e prestação de contas (HISSA; GALAMBA, 2019, p. 119).

Ana Frazão (2019, 679/685) indica que, para a estruturação de um programa de compliance, devem ser atendidos os seguintes requisitos essenciais: i) avaliação contínua de riscos e atualização do programa; ii) elaboração de códigos de ética e conduta; iii) organização compatível com o risco da atividade; iv) comprometimento da alta administração; v) autonomia e independência do setor de compliance; vi) treinamentos periódicos; vii) criação de cultura corporativa de respeito à ética e às leis; viii) monitoramento constante dos controles e processos, inclusive para fins de atualização contínua do programa; ix) canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes; e x) detecção, apuração e punição de condutas contrárias ao programa de compliance.

Inobstante, é importante lembrar que, conforme disposto no art. 42 da LGPD, na hipótese de o Poder Público ensejar danos aos titulares, qualquer que seja a natureza, possui o dever de reparação e, por outro lado, "todo tratamento de dados feito em

desacordo com a lei ou com regulamentos expedidos pela ANPD (conforme lhe é autorizado pelo art. 55-J, XIII da LGPD) é ilícito" (CURY, 2020, p. 139).

Todavia, considerando as disposições específicas para o tratamento de dados pelo Poder Público, para a aplicação de eventuais responsabilizações também se revela necessário uma adaptação da sistemática sancionatória, tendo a legislação apontado regramento específico em seus artigos 31 e 32 (FRAZÃO; DE CARVALHO; MILANEZ, 2022, p. 235/236).

E, complementa-se para a aplicação das penalidades o disposto no art. 37, §6º da Constituição Federal e arts. 189, 927, 930 e 931 do Código Civil, podendo-se o Poder Público, em eventual indenização ensejada pelo uso e tratamento irregular realizado pelas ferramentas tecnológicas que aplicam a inteligência artificial, valer-se do direito de regresso.

Além disso, conforme publicado pela ANPD na pesquisa acerca das Cidades Inteligentes supramencionada, se revelando como medidas para mitigação dos riscos ensejados à proteção de dados: i) elaboração de programa de privacidade consistente, o qual estabeleça, por exemplo, políticas, procedimentos que garantam prestação de contas, controles de acessos, auditabilidade e gerenciamento; ii) priorização de segurança cibernética na implementação de tecnologias, com exigência de padrões de tecnologia, monitoramento e controles de acessos de rede, avaliações regulares de riscos e criptografia dos dados; iii) transparência e consentimento, pelo qual deve ser promovida uma conscientização da comunidade e opções devem ser fornecidas para que os indivíduos participem dos processos; iv) armazenamento local dos dados, evitando tráfego integral dos dados na rede; v)minimização dos dados, tratando apenas as informações necessárias às finalidades previstas; vi) seja realizada a gestão de fornecedores, com seleção e supervisionamento de forma diligente das empresas parceiras e fornecedoras de serviço, com previsão de cláusulas contratuais de mecanismos de proteção e segurança da informação; vii) privacy by design, ou seja, o conceito de privacidade desde a concepção deve ser integrar desde o início do

desenvolvimento, tendo o princípio da privacidade e proteção de dados em todas as etapas do processo; viii) adotar técnicas de anonimização e pseudoanonimização de dados; e ix) medidas antidiscriminatórias com a gestão sobre a contratação e implementação das medidas oferecidas.

Assim, a proteção dos titulares das informações tratadas pelos sistemas de inteligência artificial nas cidades inteligentes e observância às disposições da LGPD implica na necessidade de atendimento para que, inclusive, assegure aos cidadãos o livre desenvolvimento e exercício da cidadania, protegendo-lhe, ainda, contra abusos e atos por domínio das informações pessoais.

Conclusão

A conclusão deste estudo ressalta a necessidade de questionar a retórica hegemônica das cidades inteligentes, impondo um exame crítico à lógica econômica contemporânea que se baseia na troca de dados pessoais por serviços (ZUBOFF, 2021). Dados são inseridos em um sistema econômico que os vê como peças em uma engrenagem destinada a extrair a solução mais lucrativa. Assim, é papel da sociedade questionar como as empresas operam nas cidades inteligentes e cabe ao Poder Público implementar e fiscalizar as leis de proteção de dados, tanto em sua atuação quanto na das empresas.

Este tensionamento entre os polos – sociedade, Estado e mercado – deve ser visto como positivo, promovendo um debate sobre a melhor forma de equilibrar a "inteligência" urbana com a proteção de dados pessoais. Para alcançar esse equilíbrio, são necessários mecanismos jurídicos e organizacionais, como a implementação de obrigações da LGPD, a nomeação de encarregados de dados, a promoção da confiança e transparência cidadã, e a defesa do direito à cidade.

Apesar da importância das ferramentas de IA e dos investimentos para transformar as cidades em ambientes mais inteligentes e aprimorar os serviços à população em áreas como saúde, educação, mobilidade urbana e segurança, é crucial que a implementação dessas tecnologias respeite o ordenamento jurídico. Devem ser selecionadas

estritamente aquelas que protejam os dados pessoais e a privacidade dos cidadãos.

Assim, destaca-se a importância da criação de normas que protejam e garantam o direito da personalidade, como as contidas no projeto de alteração do Código Civil, atuando como mecanismos de proteção da privacidade e do direito à personalidade dos cidadãos. Isso assegura que a individualidade seja mantida e o poder de autodeterminação informacional seja respeitado, sem, contudo, obstruir a inovação.

Referências

BIONI, B. R. *Proteção de dados pessoais, a função e os limites do consentimento*. Ed. Forense. Rio de Janeiro. 2019.

BERNARDINI, F.; BARCELLOS, R.; CRUZ, M. M. da. *Inteligência Artificial no Governo Eletrônico em Cidades Inteligentes: Possibilidades e Desafios*. Computação Brasil, [S. l.], n. 43, p. 27–30, 2020. DOI: 10.5753/compbr.2020.43.1793. Disponível em: https://journals-sol.sbc.org.br/index.php/comp-br/article/view/1793. Acesso em: 20.06.2024.

BRASIL. *Lei n.º 13.709 de 14 de agosto de 2018*. Poder Executivo, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 12.07.2020

BRASIL. *Parecer nº 1 da subcomissão de direito digital da CJCODCIVIL*. Senado Federal, 2023.

BRASIL. *Cidades inteligentes: radar tecnológico*. ANPD: publicação eletrônica. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf. Acesso em 20.06.2024

CURY, A. A. R. *A responsabilidade do Estado no tratamento de dados pessoais por órgãos públicos*. ***In*** Lei Geral de Proteção de Dados: Ensaios e controvérsias da Lei 13.709/18. Coord. MONACO, G.F.C.; MARTINS, A.C.M.S.; e DE CAMARGO, S. São Paulo: Quartier Latin, 2020, p. 135/142.

FRAZÃO, A. *Objetivos e alcance da Lei Geral de Proteção de Dados*. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Coord.). Lei Geral de Proteção de Dados pessoais e suas repercussões no direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019.

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.

FRAZÃO, A.; DE CARVALHO, A. P; MILANEZ, G. *Curso de Proteção de dados pessoais: fundamentos da LGPD*. Rio de Janeiro: Forense, 2022.

HISSA, C.B.; GALAMBA, P.H. N.. *O impacto da LGPD na aplicação das normas de compliance*. In. Coord. LIMA, A.P. M. C.; et al. Direito Digital: debates contemporâneos. 1ª ed., São Paulo: Thomson Reuters Brasil, 2019.

IBGE. *De 2010 a 2022, população brasileira cresce 6,5% e chega a 203,1 milhões*. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/37237-de-2010-a-2022-populacao-brasileira-cresce-6-5-e-chega-a-203-1-milhoes#:~:text=Em%202022%2C%20as%20concentra%C3%A7%C3%B5es%20urbanas,viviam%20em%20cidades%20desse%20porte. Acesso em 20.07.2024.

LEMOS, A. *Cidades inteligentes: de que forma as novas tecnologias – como a computação em nuvem, o big data e a internet das coisas – podem melhorar a condição de vida nos espaços urbanos?* In Cidades inteligentes, Gvexecutivo, v. 12, v. 2, Jul/Dez 2013, p. 46/49. Disponível em https://periodicos.fgv.br/gvexecutivo/article/view/20720/19454>. Acesso em 20.07.2024.

ONU. *World cities report 2022: Envisaging the Future of Cities*. Disponível em: <https://unhabitat.org/sites/default/files/2022/06/wcr_2022.pdf>. Acesso em 20.07.2024.

PRADO FILHO, F.O.A. *Cidades inteligentes e o direito à privacidade, uma discussão necessária. In* Direito público digital [livro eletrônico]: o Estado e as novas tecnologias: desafios e soluções Coord. RAIS, D.; PRADO FILHO, F.O.A. São Paulo: Thomson Reuters Brasil, 2020. Page: RB-3.1 Disponível em: https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/245110557/v1/page/RB-3.1%20; Acesso em 20.06.2024.

RECH, A.U. *Inteligência artificial, meio ambiente e cidades inteligentes*. Caxias do Sul: Educs, 2020. Disponível em: < https://www.ucs.br/educs/arquivo/ebook/inteligencia-artificial-meio-ambiente-e-cidades-inteligentes/>. Acesso em 20.06.2024.

RICHARDSON, Roberto Jarry. *Pesquisa Social, métodos e técnicas*. São Paulo: Atlas S. A., 1.999.

RODOTÀ, S. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

TELLES, A. *Cinco aplicações da inteligência artificial nas Smart Cities*. (eletrônico), 2023. Disponível em: <https://isaebrasil.com.br/inteligencia-artificial/>. Acesso em 20.07.2024.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy.* Harvard Law Review, Vol. 4, Nº. 5. 1890.

WEISS, M.C.; BERNARDES, R.C.; CONSONI, F.L. *Cidades inteligentes: casos e perspectivas para as cidades brasileiras.* In. Revista Tecnológica da Fatec Americana, vol. 05, n. 01, out-206/mar-2017, 01/13. Disponível em: < https://fatec.edu.br/revista/index.php/RTecFatecAM/issue/view/10>. Acesso em 22.07.2024.

WIMMER, M. *Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. **In*** Revista do Advogado. coord. BIONI, B.R. Ed.º 144, nov 2019, p. 126/133.

ZUBOFF, S. *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).

Qualificação

Isabella Souza Rainho de Oliveira Poli – ORCID 0009-0006-4348-2128
Mestranda em Ciência, Tecnologia e Sociedade pela UFSCAR. Especialista em Processo Civil pela Faculdade de Direito de Ribeirão Preto Universidade de São Paulo (FDRP/USP).
Lattes: http://lattes.cnpq.br/0753923761260320
Email: isabella@linserainho.com.br

Paloma Fernandes Lins Barca – ORCID 0009-0009-1596-3225
Especialista em Ética empresarial: direito societário, contratos e compliance pela Faculdade de Direito de Ribeirão Preto Universidade de São Paulo (FDRP/USP).
Lattes: http://lattes.cnpq.br/6177430038344105
Email: paloma@linserainho.com.br.