VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO URBANÍSTICO, CIDADE E ALTERIDADE

D597

Direito urbanístico, cidade e alteridade [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Ana Flávia Costa Eccard; Janaína Rigo Santin; Valmir Cesar Pozzetti. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-166-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito urbanístico. 3. Cidade e alteridade. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

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

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO URBANÍSTICO, CIDADE E ALTERIDADE

Apresentação

A edição do VIII ENCONTRO VIRTUAL DO CONPEDI, nos ofereceu produções cientificas inestimáveis, no âmbito do Direito Urbanístico, Cidade e Alteridade. Os trabalhos apresentados abordam uma conjuntura de temas e ideias necessárias à reflexão da comunidade cientifica sobre os problemas urbanos e as possíveis soluções. Dentro deste contexto, as apresentações realizadas no Grupo de Trabalho - DIREITO URBANÍSTICO, CIDADE E ALTERIDADE I – no dia 28 de junho de 2025, constatou-se qualificadas contribuições para o campo das Ciências Sociais Aplicadas; além de profícuo debate de todos os presentes na sala. As apresentações abordaram diferentes temáticas relativas ao meio ambiente urbano, expondo problemáticas e sugestões de crescimento humano e desenvolvimento sustentável dentro destas áreas. O GT "Direito Urbanístico, Cidade e Alteridade I", foi coordenado pelos professores doutores: Ana Flávia Costa Eccard (Centro Universitário Unifacvest); Janaína Rigo Santin (Universidade de Passo Fundo) e Valmir César Pozzetti (Univ. Federal do Amazonas e Univ. do Estado do Amazonas), que estimularam o debate e a participação de todos os presentes. A obra que ora apresentamos reúne os artigos selecionados através do sistema de dupla revisão cega por avaliadores ad hoc, de modo que temos certeza de que os temas a seguir apresentados são instigantes e apresentam significativas contribuições para as reflexões dos Programas de Pós-graduação em Direito reunidos no CONPEDI. Os trabalhos iniciaram-se com as apresentações de Ana Paula dos Santos Ferreira, Daniella Maria Dos Santos Dias, que apresentaram o trabalho intitulado "A ESPOLIAÇÃO URBANA E O ACESSO À SAÚDE: IMPACTOS DA DILAPIDAÇÃO DA FORÇA DE TRABALHO NO ACESSO À SAÚDE DA POPULAÇÃO DE BAIXA RENDA" que discutiu as possíveis intervenções do Estado para garantir o direito à saúde e buscar soluções para mitigar os impactos da espoliação urbana. Já

cumprem a sua função social e nem promovem a dignidade da pessoa humana, sendo necessário, ações mais efetivas do Poder Público municipal, uma vez que a fiscalização está ineficaz, culminando numa fragilização da democracia. Já o trabalho de Rogerio Borba, Maria Eduarda Xavier Beltrame e Ana Flávia Costa Eccard, intitulado "A PERPETUAÇÃO DA SEGREGAÇÃO RACIAL NO ESPAÇO URBANO: REFLEXÕES À LUZ DO PRINCÍPIO DA IGUALDADE", destacou que legado de séculos de discriminação e exclusão continua nas desigualdades socioeconômicas e raciais, dificultando o alcance da efetiva justiça social e a construção de um ambiente social mais igualitário. O trabalho "ACESSO A SERVIÇOS PÚBLICOS DE E-GOV COMO DIREITO FUNDAMENTAL: RISCO DE APOROFOBIA DIGITAL" de autoria de Luciana Cristina de Souza, trouxe a visão aprofundada de como a internet se mostra essencial para a concretização dos direitos da dignidade humana, evidenciando que as assimetrias sociais de acesso energético e a recursos informáticos pelos mais pobres causa sua exclusão, pois estes não conseguem usufruir dos meios tecnológicos da mesma forma que aqueles que podem arcar com o custo constante de novos equipamentos e sistema. Na pesquisa intitulada "CIDADE STANDARD E O FENÔMENO DO SUPERENDIVIDAMENTO DOS IDOSOS: CASO-REFERÊNCIA DA INCIDÊNCIA DA LEI 14.181/2021 NA PROTEÇÃO DO HIPERVULNERÁVEL NO TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO", os autores José William Marcelino da Silva, Maria Amélia Prado Fontoura, Vívian Alves de Assis, a partir de uma abordagem interdisciplinar, realizam o diálogo entre os campos do Direito e do Urbanismo na perspectiva da proteção do mínimo existencial, especialmente no que tange à quitação de dívidas de idosos via crédito consignado. Já na pesquisa "CIDADES INTELIGENTES E PRIVACIDADE: ENTRE A INOVAÇÃO E A SALVAGUARDA DE DIREITOS" os autores Pablo Martins Bernardi Coelho, Cildo Giolo Junior e Moacir Henrique Júnior constataram algumas lacunas normativas, ausência de protocolos públicos claros e riscos de discriminação algorítmica, especialmente contra os grupos vulneráveis, concluindo que há a necessidade de fortalecimento das políticas públicas de proteção informacional e adoção de uma cultura institucional de "Privacy by Design" como condição para a transformação digital urbana. No mesmo sentido, a pesquisa intitulada "CIDADES SUSTENTÁVEIS, SMART

URBANAS E DISPUTAS DE SENTIDO". Sabrina Lehnen Stoll, Ana Maria Foguesatto e Elenise Felzke Schonardie defendem que, embora se apresentem como referências de modernidade e sustentabilidade, as cidades-vitrines tendem a reforçar desigualdades socioespaciais e operar sob uma lógica de marketing urbano, despolitizando as agendas ambientais e priorizando a imagem em detrimento de transformações estruturais. Já na pesquisa intitulada "DIREITO À MORADIA, DÉFICIT HABITACIONAL E DESIGUALDADE SOCIAL NO BRASIL: UMA ANÁLISE A PARTIR DA PERSPECTIVA RACIAL" as autoras Carina Lopes de Souza e Elenise Felzke Schonardie questionam a forma como o cenário urbano se configuram, no Brasil, concluindo que o cenário urbano e habitacional é marcado pela segregação socioespacial, cujos efeitos incidem de maneira mais acentuada sobre a população preta e parda. Seguindo uma linha de raciocínio semelhante, Adriana Vilhena Karlsson, Ana Manoela Piedade Pinheiro e Daniella Maria Dos Santos Dias, na pesquisa intitulada "ESPOLIAÇÃO URBANA E DIREITO À CIDADE: O CASO DAS COMUNIDADES DO ENTORNO DO ATERRO DE MARITUBA"concluem que há uma disparidade entre o ideal normativo do Direito à Cidade e a realidade concreta de exclusão socioambiental, na qual populações vulneráveis são forçadas a residir em áreas insalubres, desprovidas de infraestrutura e dignidade urbana. Já a pesquisa intitulada "IMPACTOS DAS MUDANÇAS CLIMÁTICAS NAS CIDADES: UMA ANÁLISE CRÍTICA DAS POLÍTICAS PÚBLICAS" de autoria de Fátima Cristina Santoro Gerstenberger, Isabella Franco Guerra e Maíra Villela Almeida, concluíram que a formulação de políticas públicas eficazes demanda uma abordagem multidisciplinar, colaborativa e fundamentada em dados científicos, com ampla participação social. A construção de cidades resilientes e ambientalmente inteligentes foi apontada como caminho fundamental para enfrentar os desafios climáticos e promover um futuro urbano mais sustentável e equitativo. Já a pesquisa intitulada "IMPROBIDADE ADMINISTRATIVA E ESTATUTO DA METRÓPOLE: IMPACTO DO VÁCUO LEGISLATIVO NA PROTEÇÃO DA POLÍTICA DE GOVERNANÇA INTERFEDERATIVA EM MATÉRIA URBANÍSTICA" de autoria de Emerson Affonso da Costa Moura, Mauricio Jorge Pereira da Mota e Marcos Alcino de Azevedo Torres, faz uma análise sobre a necessidade de se eliminar a suposta

por cidades mais resilientes, não é aceitável a ideia da supressão das poucas áreas verdes que ainda restam nos meios urbanos. Numa linha de raciocínio semelhante, os autores Fátima Cristina Santoro Gerstenberger, Otto Guilherme Gerstenberger Junior e Guilherme Santoro Gerstenberger, na pesquisa intitulada "O DIREITO À PROPRIEDADE IMOBILIÁRIA COMO DIREITO FUNDAMENTAL: ANÁLISE CONSTITUCIONAL" também destacam a necessidade de o meio ambiente urbano ser sustentável e que as Políticas Públicas assegurem que a propriedade urbana cumpra a sua função social. Já Valdemiro Adauto de Souza, na pesquisa "OPERAÇÕES URBANAS CONSORCIADAS: INSTRUMENTO DOS MUNICÍPIOS PARA EDIFICAÇÃO DE CIDADES SUSTENTÁVEIS", destaca as Operações Urbanas Consorciadas como instrumento para edificação de Cidades Sustentáveis, bem como a necessidade de haver uma integração e compreensão dinâmica (e eficaz) desse instrumento de política urbana tendo como ponto de partida a função social do Estado (e dos Municípios) Contemporâneo. Na pesquisa intitulada "POSSO ME ENCOSTAR?: A DIFICULDADE DE DEFINIÇÃO DAS TÉCNICAS CONSTRUTIVAS HOSTIS A PARTIR DA EDIÇÃO DA LEI PADRE JÚLIO LANCELOTTI", os autores Lucas Manito Kafer, Agna Valim Cardoso e Daniela G. Vilela investigam os desafios enfrentados pelos municípios gaúchos para a implementação e fiscalização da Lei nº 14.489/2022, conhecida como Lei Padre Júlio Lancelotti, que proíbe o uso de técnicas construtivas hostis em espaços públicos. Buscando evidenciar a problemática da regularização fundiária na Amazônia, as autoras Ana Luisa Santos Rocha e Luly Rodrigues Da Cunha Fischer, na pesquisa "QUESTÃO FUNDIÁRIA E REGISTRAL NA AMAZÔNIA: A ANÁLISE DE UMA CADEIA DOMINIAL NO MUNICÍPIO DE PARAUAPEBAS/PA" discutem a questão fundiária e registral na Amazônia e os desafios enfrentados na análise do direito de propriedade imobiliária a partir da elaboração de cadeias dominiais. Já o trabalho intitulado "TELESSAÚDE E RELAÇÃO PROFISIONAL-PACIENTE: UMA PERSPECTIVA ÉTICA E JURÍDICA", de autoria de Janaina Rigo Santin e Sandy Mussatto, explora a contratação de serviços de saúde, por municípios do interior do estado de ..... onde o custo é mais barato e o acesso à telemedicina se faz através da internet, mas a pesquisa questiona a qualidade destes serviços (Janaina você via precisar fazer um breve resumo do seu trabalho).

Centro Universitário Unifacvest

Profa. Dra. Janaína Rigo Santin

Universidade de Passo Fundo

Prof. Dr. Valmir César Pozzetti

UEA e UFAM

CIDADES INTELIGENTES E PRIVACIDADE: ENTRE A INOVAÇÃO E A SALVAGUARDA DE DIREITOS

SMART CITIES AND PRIVACY: BETWEEN INNOVATION AND THE SAFEGUARDING OF RIGHTS

Pablo Martins Bernardi Coelho [1]
Cildo Giolo Junior [2]
Moacir Henrique Júnior [3]

Resumo

Esta pesquisa estuda a relação de impacto entre as smart cities brasileiras e o tratamento dos dados pessoais dos indivíduos. Demonstra conceitos e desenvolvimentos das cidades inteligentes, além dos estudos de jurisdições que resguardam o direito a privacidade. Foi possível tecer variadas proposições sobre como são tratados os dados pessoais coletados pelas novas tecnologias das cidades inteligentes e quais os métodos que as administrações públicas deveriam adotar para evitar a violação da privacidade dessas informações,bem como pontuadas possíveis ações públicas para resguardar o direito do cidadão. Assim, analisou-se a relação entre o desenvolvimento das cidades inteligentes brasileiras e os desafios à efetividade do direito fundamental à privacidade, diante do crescente uso de tecnologias de coleta e tratamento de dados pessoais. Parte-se da constatação de que a governança digital urbana, embora promova avanços em mobilidade, segurança e gestão pública, pode comprometer garantias constitucionais quando implementada sem salvaguardas adequadas. O objetivo central é avaliar até que ponto os mecanismos legais têm sido eficazes na proteção das informações dos cidadãos em contextos urbanos tecnologizados. A metodologia empregada estrutura-se na análise dogmático-jurídica dos dispositivos normativos que tratam da proteção de dados pessoais no Brasil e no estudo de casos concretos de cidades brasileiras que se autodenominam inteligentes. Revelou-se algumas lacunas normativas, ausência de protocolos públicos claros e riscos de discriminação algorítmica, especialmente contra grupos vulneráveis. Conclui-se pela necessidade de fortalecimento das políticas públicas de proteção informacional e adoção de uma cultura institucional de “Privacy by Design” como condição

Palavras-chave: Cidades inteligentes, Privacidade, Proteção de dados pessoais, Governança digital, Políticas públicas

Abstract/Resumen/Résumé

This research examines the impact relationship between Brazilian smart cities and the processing of individuals' personal data. It presents concepts and developments related to smart cities, as well as studies of jurisdictions that safeguard the right to privacy. Various propositions were formulated on how personal data collected by smart city technologies are handled, and which methods public administrations should adopt to prevent privacy violations, including potential public actions to protect citizens' rights. The study analyzes the link between the development of Brazilian smart cities and the challenges to the effectiveness of the fundamental right to privacy in light of the growing use of data collection and processing technologies. It is based on the understanding that, while digital urban governance fosters progress in mobility, security, and public management, it may also compromise constitutional guarantees when implemented without adequate safeguards. The main objective is to assess to what extent legal mechanisms have been effective in protecting citizens' information in technologized urban contexts. The methodology is based on a dogmatic-legal analysis of the Brazilian legal framework on personal data protection, along with case studies of Brazilian cities that identify as smart cities. The study revealed normative gaps, lack of clear public protocols, and risks of algorithmic discrimination, particularly against vulnerable groups. It concludes that strengthening public information protection policies and adopting an institutional culture of "Privacy by Design" are essential for legitimate digital urban transformation.

Keywords/Palabras-claves/Mots-clés: Smart cities, Privacy, Personal data protection, Digital governance, Public policies

1 INTRODUÇÃO

> Vivemos num tempo em que as questões relacioandas à proteção de dados pessoaos se caracterizam por uma abordagem marcadamente contraditória – de fato, uma verdadeira esquizofrenia social, política e institucional. Tem-se aumentado a consciência dda importância da proteção de dados o que se refere não só à proteção das vidas privadas dos indivíduos, mas a sua prórpia liberdade. (Rodotà, 2007, p. 11)

As chamadas cidades inteligentes, ou smart cities, surgem do avanço acelerado das tecnologias digitais e representam um novo tipo de organização urbana, que utiliza ferramentas tecnológicas como base para melhorar a qualidade de vida dos moradores, aumentar a segurança pública e promover o crescimento social e econômico das áreas onde são implantadas. Esta proposta se apoia no uso de dispositivos eletrônicos interconectados que permitem o registro e a análise contínua de dados em toda a cidade. As informações são aproveitadas para pensar soluções que respondam a desafios em áreas como saúde, mobilidade, educação, segurança e economia.

No entanto, apesar dos ganhos prometidos, o processo de captação e uso de dados levanta preocupações legítimas sobre a proteção da privacidade individual, como já alertava a sociedade cosmopolita de risco de Beck (2013). Afinal, o uso constante de dados pessoais, pode abrir espaço para abusos ou uso indevido dessas informações, colocando em risco o direito da privacidade.

Em razão disso, esta pesquisa busca examinar, no contexto das cidades inteligentes no Brasil, como tem se dado a proteção do direito à privacidade dos cidadãos diante da coleta de dados pessoais. Pretende-se avaliar se os mecanismos adotados têm sido eficazes e suficientes para garantir esse direito, considerando as exigências dos regulamentos de salvaguarda pátrios e os desafios práticos de sua aplicação em ambientes urbanos digitalizados.

Em que medida, os mecanismos de governança de dados e as políticas públicas, que estruturam as cidades inteligentes brasileiras, asseguram, na prática, a efetividade do direito fundamental à privacidade previsto? Esse estudo propõe uma análise sobre a necessidade de um tratamento responsável, transparente e ético desses dados, destacando-se até que ponto que a segurança individual deve ser comprometida em nome da segurança pública e do progresso tecnológico.

Esta investigação adotou um desenho metodológico estruturado em dois pilares complementares que dialogam de forma orgânica, utilizando primeiramente do método dogmático-jurídico, para estudar o regime de proteção de dados aplicável onde foram

examinados, em perspectiva integrativa, a Constituição Federal (art. 5º, XII e LXXIX), a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011) e atos infralegais (Resoluções ANPD n.º 2/2022 e 4/2023, entre outras).

Esta análise identificou a necessidade de políticas públicas capazes de condicionar a coleta, o tratamento e o compartilhamento de dados pelo poder público local e por parceiros privados que operam soluções urbanas inteligentes, com o intuito de respeitar os princípios e deveres legais.

Posteriormente, consistiu em estudos de casos exemplificativos, que foram selecionados, por critérios de relevância e disponibilidade de informação, cidades que se autodenominam inteligentes e mantêm iniciativas consolidadas de vigilância ou gestão de dados urbanos.

2 DIREITO A PRIVACIDADE

O direito a privacidade é um composto de garantias e normas a quais são responsáveis por assegurar a privacidade de cada indivíduo, para que esta não seja violada pelo estado ou por particulares. Assim, este direito constitucional presente no art. 5º da Constituição Federal, no art. 21 do Código Civil, na Lei Geral de Proteção de Dados Pessoais, e em outras diversas normas especiais garante o resguardo da vida particular e privada do indivíduo.

O objetivo deste direito é a proteção da personalidade humana e segurança do indivíduo como denominado pelo Juiz Cooley "o direito de estar só", de acordo com artigos publicados dos autores Samuel Warren e Louis Brandeis. Segundo eles, as fotografias e as empresas de comunicação com suas novas tecnologias têm invadido o espaço do lar (Warren; Brandeis, 1890). De acordo com os autores o direito à privacidade não seria considerado como um direito proprietário, visto que o direito de estar só seria uma das instâncias para a tutela de pensamentos e sentimentos.

2.1 Conceito de Privacidade

> They conferred, as against the Government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. (United States, 1928)[1].

[1] "Eles conferiram, em face do Governo, o direito de ser deixado em paz — o mais abrangente dos direitos e o direito mais valorizado pelos homens civilizados." (Tradução nossa)

O direito à privacidade no século XX, foi se desenvolvendo devido a relação do indivíduo com os espaços públicos e privados, devido a isso ocorreu significativas mudanças por estimular a democracia do direito à privacidade e seu exercício. Logo, essa norma se expande para novos sujeitos, objetos e locais, anteriormente incompatíveis.

Em uma linha mais tradicional americana, o doutrinador Tércio Sampaio Ferraz Jr. em seu resumo sobre o sigilo dos dados pessoais destaca que:

> A privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (ou estar-só), o segredo, a autonomia. Na intimidade protege-se sobretudo o estar-só; na vida privada, o segredo; em relação à imagem e à honra, a autonomia. (Ferraz Jr., 1993. p. 439).

Em relação a isso, o autor defende que o direito à privacidade corresponde a um direito subjetivo fundamental. Logo, desenvolve uma estrutura básica, o qual classifica os elementos em sujeito, conteúdo e objeto.

> O sujeito é o titular do direito. (...) é toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente (ou transeunte [...]) no País (art. 5º, caput). O conteúdo é a faculdade específica atribuída ao sujeito, que pode ser a faculdade de constranger os outros ou de resistir-lhes (caso dos direitos pessoais) ou de dispor, gozar, usufruir (caso dos direitos reais). A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão. O objeto é o bem protegido, que pode ser uma res (uma coisa, não necessariamente física, no caso de direitos reais) ou um interesse (no caso dos direitos pessoais). No direito à privacidade, o objeto é, sinteticamente, a integridade moral do sujeito. (Ferraz Jr., 1993, p. 440)

Nota-se que o autor é adepto da doutrina estadunidense em relação ao direito à privacidade, na qual o direito ao isolamento era matriz da doutrina do “Right to Privacy”.

Entre nós, a doutrina brasileira é resultante da doutrina italiana, pois esta determinou que o direito a privacidade vai além do “direito de ser deixado só”, como citado por Carlo Colapietro:

> O caráter complexo deste direito se manifesta concretamente em dois perfis: a primeiro mais geral e clássica prerrogativa à não interferência, na sua conhecida acepção de “right to be let alone”; o segundo, ao invés, coincide com a ideia de autorrealização, com ser patrão de si, ou, com o ser, em potência, aquele que projeta a vida na própria sociedade, que forja a sua história. (*apud* Colombo; Berni, 2022, p. 21)

Dessa forma, a doutrina italiana demonstrou preocupação com a dignidade da pessoa humana diante dos avanços tecnológicos, ao destacar o princípio da autodeterminação

informativa, entendido como o direito do indivíduo de exercer controle sobre seus próprios dados pessoais, especialmente no sentido de decidir como suas informações serão utilizadas.

Contudo, diferente das doutrinas anteriores, o legislador brasileiro ao formular a Constituição de 1988 e o Código Civil de 2002, escolheu identificar expressamente a diferença dos diversos sentidos do termo privacidade, não utilizando desse vocábulo, mas substituindo pelos termos vida privada e intimidade. Ademais, a Constituição também acrescentou as expressões sigilo e inviolabilidade da casa.

Assim, privacidade, deve ser entendida primordialmente como o exercício da liberdade de um indivíduo, uma exigência humana a qual faz parte internamente para sua formação. Ter privacidade é essencial tanto no estar só como no entendimento contemporâneo do controle de informações.

O direito à intimidade está inserido na expressão direito à privacidade, como descrito no entendimento de Cabral "grau de proteção da intimidade em uma dada situação poderá variar de acordo com elementos objetivos casuísticos" (2012, p. 116). Logo:

> [...] resguardo da reserva varia na medida em que os fatos se situem no ciclo de sigilo, de resguardo ou de publicidade da vida do indivíduo. Tudo depende de tudo. Das pessoas, de cada pessoa, da sua sensibilidade e das suas circunstâncias; nas necessidades e exigências da sociedade relativas ao conhecimento e à transparência da vida em comum. (2012, p. 116-117)

Assim, o direito à privacidade, previsto na Constituição e na legislação infraconstitucional, é considerada direito fundamental e direito da personalidade. Logo, é uma figura jurídica, a qual excede a divisão entre direito público e privado,

A proteção a privacidade, tem como um de seus objetivos contemplar "atributos da personalidade humana merecedores de proteção jurídica", assim dizendo, o que "muda é tão somente o plano em que a personalidade humana se manifesta" (Schreiber, 2013, p. 13). Consistindo, dessa forma, a privacidade como constituinte fundamental para a formação do indivíduo, sendo indispensável para a construção da pessoa e suas fronteiras com todos a sua volta (Doneda, 2021), ou seja, sua proteção vai de encontro com a tutela a dignidade da pessoa humana, princípio este norteador do ordenamento jurídico pátrio.

A Constituição Federal de 1988, tem enunciados que referem-se sobre a tutela a privacidade, sendo eles no art 5º, em seus incisos X, XI, XII e XIV, que preveem, respectivamente:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à

> propriedade, nos termos seguintes: [...]
> 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;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; [...]

Em suma, a privacidade esta ligada historicamente a tutela da propriedade e do direito relacionado aos seus bens, e intimidade faz referência a proteção do livre desenvolvimento e cautela da personalidade.

2.2 O direito à privacidade na sociedade em rede

Com o avanço tecnológico no século XX e a valorização da informação, ficou mais fácil deacessar dados privados e divulgá-los, este que será para toda a coletividade. Devido a isso, a privacidade deixou ser exclusiva, e em 1948 a Declaração Universal dos Direito Humanos determinou "[...] ninguém sofrerá intromissões arbitrárias na sua vida privada". Entretanto, foi na última década do século XX com o surgimento da internet a qual elevou-se a interação entre as comunidades e cresceu a circulação de informações na assim chamada Sociedade em Rede. Esse termo referente à sociedade atual foi inicialmente cunhado pelo sociólogo holandês Jan Van Dijk (1991), e amplamente popularizado e aprofundado pelo sociólogo espanhol Castells (1999), sendo que este explorou como as redes digitais transformaram a economia, a cultura e as relações sociais, tornando-se uma referência essencial no estudo da era da informação.

Solove afirma que a privacidade, contudo, "é um conceito em desordem", pela amplitude que o termo comporta. Essa observação não é mera retórica, a indefinição mina a capacidade do direito e das políticas públicas de tratar coerentemente das novas ameaças que surgem na sociedade da informação.

> Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. Philosophers, legal theorists, and jurists have

> frequently lamented the great difficulty in reaching a satisfying conception of privacy. (2008, p. 2)[2]

O primeiro elemento causador dessa entropia é a própria elasticidade do termo. Ao longo do tempo, teorias rivais converteram "privacidade" em rótulo para fenômenos muito distintos, como controle sobre dados pessoais, intimidade sexual, anonimato, inviolabilidade do domicílio, sem, contudo, oferecer um traço comum que mantenha o conceito coeso. O resultado é que a palavra parece significar tudo e, ao mesmo tempo, nada de específico; carece de fronteiras nítidas e se dissolve em múltiplas acepções.

O segundo problema é a ausência de consenso entre filósofos, juristas e sociólogos. Solove recorre a vozes de peso para mostrar que, apesar de décadas de debate, não se consolidou uma definição minimamente estável. Cada escola de pensamento enfatiza um aspecto diferente e critica as demais por serem vagas, estreitas ou contraditórias. Como se não bastasse, o espaço público é invadido por metáforas alarmistas. Livros, reportagens e decisões judiciais repetem que a privacidade estaria morrendo, enquanto outros autores a consideram um valor antissocial, supérfluo ou mesmo nocivo à transparência coletiva. (Solove, 2008, p.15-25).

Atualmente, os interesses privados e públicos estão sendo considerads justificativas plausíveis para a constante violação a privacidade do cidadão. Entretanto, respeitar o direito à privacidade é exercer o exercício da cidadania indispensável, visto que a [...] poluição das liberdades civis não é menos importante que a poluição do meio ambiente" (Rodotà, 2007, p. 20).

3 CIDADES INTELIGENTES

Cidades inteligentes são espaços urbanos inovadores os quais tem como objeto central seu processo de planejamento a tecnologia, utilizado de modo generalizado em sua gestão e seus recursos por meio de ideias criativas, sustentáveis e com a colaboração da população para a infraestrutura do ecossistema. As inovações e a tecnologia são utilizadas para melhorar a qualidade da vida urbana.

Em razão desse novo formato de governança urbana ser administrado pela tecnologia e devido ao desenvolvimento, nos últimos tempos, dos sistemas de informações, André Lemos,

[2] "Ninguém pode articular o que isso significa. Atualmente, a privacidade é um conceito abrangente, abrangendo (entre outras coisas) liberdade de pensamento, controle sobre o corpo, solidão em casa, controle sobre informações pessoais, liberdade de vigilância, proteção da reputação e proteção contra buscas e interrogatórios. Filósofos, teóricos do direito e juristas freqüentemente lamentaram a grande dificuldade em alcançar uma concepção satisfatória de privacidade." (tradução nossa).

em seu trabalho, define que as cidades são denominadas como inteligentes com base em seus dados informatizados:

> [...] inteligente refere-se a processos informatizados sensíveis ao contexto, lidando com um gigantesco volume de dados (Big Data), redes em nuvens e comunicação autônoma entre diversos objetos (Internet das Coisas). Inteligente aqui é sinônimo de uma cidade na qual tudo é sensível ao ambiente e produz, consome e distribui um grande número de informações em tempo real. (Lemos, 2014)

No que tange a redundância da origem do termo, Montefusco et al., afirmam que "Avanços tecnológicos são patentes na evolução dos meios urbanos que, ao seu turno, guardada as devidas proporções, sempre foram inteligentes." (2024, p. 2).

Neste contexto não se trata apenas em desempenhar novas tecnologias de forma irrestrita, é necessário a conscientização de que as políticas públicas devem priorizar a qualidade de vida, e não apenas o uso de sensores tecnológicos. Os conflitos urbanos não serão solucionados apenas com o uso da tecnologia em razão disso então é necessário a priorização da qualidade de vida, por meio da criatividade e esforços públicos por parte da governança das cidades inteligentes.

Hodiernamente, as cidades inteligentes são uma realidade em diversos países do mundo, Rios Neto e Gimenez (2018), relacionaram algumas como Londres, Inglaterra; Copenhague, Dinamarca; Nova York, Estados Unidos; Helsinque, Finlândia; entre outros. Entretanto, destacaram a cidade de Tóquio, capital do Japão, a qual foi considerada em 2019 a cidade mais inteligente do mundo. Nesse sentido,

> A cidade é conhecida por suas novidades tecnológicas e também futuristicas. O desenvolvimento de inovações, as eficientes medidas tomadas para controlar a quantidade de energia utilizada em suas residências e edifícios comerciais e a colaboração entre governo e as maiores empresas do Japão, como a Panasonic, Mitsubishi e Sharp, com a responsabilidade de desenvolver e difundir a tecnologia inteligente contribuem para esse avanço da cidade (Rios Neto; Gimenez, 2018, p.3).

O continente europeu tem um programa denominado de Projeto Cidades Europeias Inteligentes, o qual agrega pelo menos 70 cidades, em razão disso, Weiss (2013, p. 65) acrescenta outros nomes na lista como Mechelen, Bélgica; Groningen, Holanda; Oldenburg, Alemanha, além de outras, ele usa de exemplo Karlstad, na Suécia:

> Proporciona informações e canais de comunicação para cidadãos, visitantes e estudantes, abrangendo o sistema educacional e assistência infantil; saúde e assistência social; edificações e condições de vida urbana; ambiente, energia (geração, preservação e uso racional) e zeladoria urbana; tráfego e

> infraestrutura de transportes; negócios e trabalho; acesso pleno à internet por meio de conexões com fibra ótica e cobertura de rede sem fio em toda a cidade, e; informações e interações sobre políticas e demonstrações realizadas pelo poder público (Weiss; Bernardes; Consoni, 2015, p. 313).

O tratamento dos dados coletados pelas novas tecnologias nas cidades inteligentes causam um impasse, no qual os dados pessoais são informações essenciais para a elaboração de políticas públicas eficientes, em contrapartida, há o receio de que esse material seja utilizado para finalidades adversas ao que inicial foi proposto.

Em razão disso, Paola Salvatori Damo afirma, usando de exemplo o período da pandemia e o uso de inovadoras tecnologias para controle de deslocamento populacional:

> Nesse cenário, as medidas de utilização de tecnologias capazes de controlar e monitorar a disseminação do vírus parecem válidas e legítimas - desde que observadas as boas práticas de tratamento dos dados pessoais colhidos para que não sejam violados direitos fundamentais dos cidadãos. Ou seja, essa supervigilância decorrente da pandemia da covid-19 está diretamente ligada à proteção de dados pessoais, sendo um dos motivos influenciadores da institucionalização e da regulação do direito à privacidade (Damo, 2020)

A autora supracitada ainda pontua sobre a LGPD e sua flexibilização com o tratamento de dados devido ao caso específico do período pandêmico:

> Dentre suas bases legais, a LGPD tem explicitamente listadas a proteção da vida, da incolumidade física e a tutela da saúde. Ao contrário do que se imagina, o consentimento não é requisito absoluto para que dados pessoais sejam colhidos e tratados: ele é somente uma das hipóteses de tratamento de dados pessoais previstas no art. 7º, da lei. Já no caso do tratamento de dados sensíveis (art. 11), ele pode ser dispensado em alguns casos específicos como: (i) ser necessário para a execução de políticas públicas; (ii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; e, principalmente, (iii) para a tutela da saúde. (Damo, 2020)

Vários questionamentos emergem no que tange à captação de informações pelos entes públicos: O que será feito com os dados? Quem poderá ter acesso?. Por isso a necessidade do chamado "Privacy by Design" previsto na LGPD, o qual assegura aos titulares dos dados privacidade em todo ciclo de vida, desde o momento da coleta da informação até sua exclusão da base de dados:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> [...]
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Assim, antes dos entes governamentais pensarem em tecnologias de monitoramento da pandemia, é fundamental que estes busquem aquelas que cumpram o "Privacy by Design", mantendo altos padrões de segurança da informação e de proteção de dados.

4 UTILIZAÇÃO DE DADOS PERSONALISSIMOS PELAS CIDADES INTELIGENTES BRASILEIRAS

Segundo o Ministério da Ciência, Tecnologia e Inovações, o Brasil cresceu 6,5% em 2021 no setor de TIC. Dessa forma, os estudos estimam que em projeções futuras para 2022, o Brasil terá um aumento de 8,2% de gastos nas Indústrias de Softwares e Serviços de TIC. A consequência desse aumento será devido ao crescimento da economia digital, cenário este devido a pandemia. Assim, são necessários investimentos em segurança de dados gerados pelas novas TICs, como por exemplo as diretrizes e as atitudes da Instituições Cientificas e de Inovação Tecnologicas (ICTs):

> Em relação à atuação das ICTs, o estudo apurou que 67,9% afirmaram ter uma política de diretrizes para ações de inovação, proteção à propriedade intelectual e transferência de tecnologia e 70,3% informaram possuir pedidos de proteção requeridos ou concedidos no ano. Desses, 97,8% foram efetivados no Brasil e 2% no exterior. (Brasil, 2024)

Logo, é possível visualizar esse crescimento da economia digital, no desenvolvimento de soluções tecnológicas, adotadas rapidamente, no período pandêmico, com o intuito de promover melhorias no novo cotidiano dos cidadãos.

Todavia, essas medidas adotadas em momentos singulares podem apresentar riscos futuros, por exemplo para se evitar um desses conflitos, o Brasil suspendeu a Medida Provisória nº 954/2020, a qual tratava-se do compartilhamento de dados entre o IBGE e as empresas prestadoras serviços de telecomunicações (STF, 2020), esta decisão manifesta a necessidade do aprofundamento do debate em relação a proteção de dados no país.

Ademais, essas diversas práticas tecnológicas inovadoras, as quais interagem e interferem diretamente no tratamento dos dados pessoais, principalmente no período pandêmico, foi adotado por muitos governos dos estados brasileiros os quais desenvolveram métodos para obterem informações de, por exemplo, deslocamento populacional da cidade.

Analogamente, o Estado de São Paulo, o qual desenvolveu o SIMI-SP (Sistema de Monitoramento Inteligente de São Paulo) cuja finalidade é ser uma análise estratégica de geolocalização, sobre a população, em relação ao percentual de infectados, número de isolados,

entre outros, por cada região da cidade.

Esse programa foi desenvolvido em parceria com quatro grandes empresas de telefonia, e instituído pelo decreto estadual nº 64.963, de 5 de maio de 2020, além de ter acesso a dados de 30 mil pessoas, em relação a isso o portal do governo do Estado de São Paulo afirma:

> Com o SIMI-SP, o Governo de São Paulo pode obter informações a respeito dos percentuais de isolamento e de aglomeração vinculados a cada antena de telefonia móvel. Não há ameaça à privacidade dos usuários, uma vez que não são analisadas as trajetórias individualmente e todos os dados são anonimizados e apresentados de forma agregada. (Portal do Governo, 2020)

A prefeitura do Rio de Janeiro, em parceria com a empresa TIM, no período pandêmico, também utilizou de dados de telecomunicações para analisar os dados de deslocamento de seus cidadãos, utilizando como base um dos projetos desenvolvidos nas Olimpíadas e na Copa do Mundo na cidade. Em relação as informações pessoais coletadas, o CTIO da Tim Brasil, Leonardo Capdeville afirma que os dados de seus clientes são anonimizados "Todas as informações coletadas são anônimas, respeitando critérios de confidencialidade e segurança de dados pessoais, segundo prevê a Legislação" (Estadão Conteúdo, 2020).

Todavia, Danilo Doneda, ressalta sobre a importância do resguardo com dados pessoais mesmo em momentos de emergência:

> Estando a proteção de dados vocacionada à proteção do cidadão, a sua disciplina compreende dispositivos capazes de legitimar a utilização de seus dados pessoais em situações nas quais o seu interesse ou o da sociedade é prioritário, como ocorre em situação como a que estamos passando. (...) Este elemento fundamental que é a legitimação para o uso em situações de emergência não é, de forma alguma, uma carta em branco fornecida pelas legislações de proteção de dados para o emprego irrestrito de dados pessoais: assim como em outras situações, o seu tratamento deve respeitar direitos e garantias individuais (...) somente para a estrita finalidade de conter a emergência, a minimização de riscos através da utilização de um conjunto mínimo de dados possível, a anonimização e pseudonimização sempre que possível, o emprego das medidas de segurança necessárias.(Doneda, 2021)

Assim, tem-se o impasse no qual em meio a uma pandemia, os dados pessoais são informações essenciais para a elaboração de políticas públicas eficientes para conter o vírus, em contrapartida, há o receio de que esse material seja utilizado para finalidades adversas ao combate à doença.

Logo, as cidades inteligentes brasileiras estão em constante impasse de interesses pois um lado defende a limitação de acesso aos dados em razão da tutela a privacidade e outro lado defende o tratamento de dados como oportunidade para o desenvolvimento urbano.

4.1 Utilização de dados pessoais nas cidades inteligentes

As cidades inteligentes, entre seus elementos principais está a utilização dos dados pessoais dos cidadãos por meio das TICs com o intuito de empregar essas informações para melhorar a qualidade de vida urbana. Entretanto, a tecnologia possui efeitos maléficos, como o uso insdiscriminado e irresponsável dos dados armazenados.

Dessa forma é possível visualizar o risco do mal uso desse banco de armazenamento de dados pessoais em algumas dessas TICs aplicadas em cidades brasileiras.

O Estado de São Paulo, caracterizada como smartcity, tem entre seus projetos da administração publica o sistema "Detecta", este configura em 3 mil câmeras de vigilância que reúnem em um banco de dados de informação policiais, sendo considerado o maior da América Latina, em decorrência da correlação de informações entre polícia militar e civil, além de conhecimento de dados do Sistema Operacional da Policia Militar, Registro Digital de Ocorrências, Instituto de Identificação, entre outros.

Dessa forma, os dados dos indivíduos são coletados massivamente. A questão a ser considerada, como explicado por Doneda e Machado, é a garantia dos direitos fundamentais dos cidadãos, para que não ocorra além do descumprimento do direito à privacidade também não aconteça situações discriminatórias:

> A garantia de direitos dos cidadãos cujos dados serão coletados e processados massivamente no ecossistema de cidade inteligente ganha destaque, cada vez mais, como a questão fundamental que é e que deve ser considerada, sobretudo num contexto de crescente uso de serviços inteligentes para policiamento (preditivo).
> Além de poder causar interferências no direito à privacidade, não é novidade que a coleta dados pessoais em grande escala incrementa o risco de viés discriminatório em sistemas algorítmicos e de tomada de decisão automatizada, em especial em aplicações de policiamento preditivo e de reconhecimento facial, contra minorias e grupos vulneráveis. (Doneda; Machado, 2019, p.6).

De acordo com Pablo Nunes, coordenador do projeto do CESeC, o Panóptico, o qual tem como objetivo acompanhar o uso dessas tecnologias de reconhecimento facial para o policiamento, destaca em relação a esses encarceramentos:

> O Brasil é um dos países que tem a maior população carcerária do mundo, e das que mais cresce. E a gente não tem assistido uma melhora da nossa segurança pública nesse aumento do encarceramento, muito pelo contrário. E estamos com o reconhecimento facial fazendo uma nova aposta no encarceramento como resolução dos problemas de segurança pública do país.

(Soares, 2022).

Em razão disso, no Estado de São Paulo, está tramitando na Assembleia Legislativa o projeto de lei PL 385/2022, o qual de acordo com seu art. 3º ira vedar:

> Artigo 3º Fica vedado, nos termos desta Lei, ao Poder Público no Estado de São Paulo:
> I. Obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial ou informações derivadas de uma tecnologia de reconhecimento facial;
> II. Celebrar contrato com terceiro com a finalidade ou objetivo de obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial, informações derivadas de uma tecnologia de reconhecimento facial ou manter acesso à tecnologia de reconhecimento facial;
> III. Celebrar contrato com terceiro que o auxilie no desenvolvimento, melhoria ou expansão das capacidades da tecnologia de reconhecimento facial ou forneça ao terceiro acesso a informações que o auxiliem a fazer isso;

Outras cidades também instalaram câmeras pelas ruas de reconhecimento facial como Recife, instalou relógios digitais equipados com câmeras; no Rio de Janeiro, também instalou o projeto-piloto pela Polícia Militar de vídeo-monitoramento com reconhecimento fácil pelas ruas. Dessa forma, Nicolau Soares destaca:

> A gente não encontra uma base mínima para que esse tipo de tecnologia pudesse ser utilizada. Ou seja, protocolos operacionais, regulação, determinações claras de quem, quando e como será feito o acesso aos dados das pessoas, o ciclo de vida desses dados, quem vai ser responsável pelos erros ocorridos durante essa implementação. A gente não tem esse estudo básico. (Soares, 2022).

Ademais, Soares destaca sobre o risco do governo na adoção das tecnologias de reconhecimento facial, em diferentes espaços, não apenas no meio policial, mas também nos sistemas de auxílios governamentais, no transporte publico:

> O uso das tecnologias em espaços públicos. Há dezenas, centenas de aplicações desses algoritmos e a gente focou neles sendo operados no espaço público, porque é nesse uso que a gente encontra o maior número de violações possíveis à privacidade, aos direitos humanos e a outras garantias legais.
> Mas isso não exime do fato de que esses algoritmos podem sim produzir vieses que vão prejudicar o acesso a direitos. Se a gente pensa no Gov.br, que é uma plataforma pela qual a gente consegue acessar boa parte dos serviços operados pelo governo federal, se ele coloca esse sistema aliado ao reconhecimento facial, determinadas pessoas vão ter mais dificuldade de validar seu cadastro para acessar esses direitos. A gente viu esse processo acontecendo durante a pandemia de covid, principalmente a partir da criação do auxílio emergencial, que necessitava de validação por meio de reconhecimento facial. Isso acabou promovendo uma série de dificuldades para determinada parcela da população ter esses direitos assegurados.

(2022)

Assim, fica permitida a exploração econômica das informações coletadas do sistema de bilhetagem eletrônica dos transportes públicos. Em razão disso os autores Dannys Marcelo Antonialli e Beatriz Kira, afirmam:

> A possibilidade de comercialização dessa ampla base de dados coloca, portanto, em risco a privacidade dos mais de 15 milhões de usuários ativos da rede de transporte público da Grande São Paulo, pois forneceria à empresa dados detalhados sobre a origem e o destino dos usuários. Ademais, os dados pessoais sobre deslocamento são gerados pelos usuários e entregues à administração pública de forma involuntária, sem que estejam em vigor termos de uso que exijam a manifestação do consentimento dos munícipes e que estabeleçam regras claras a respeito de como o tratamento dessas informações se dará. (Antonialli; Kira, 2020)

Por fim, Nunes explica sobre a aplicação de toda essa tecnologia que necessita de uso de dados pessoais dos cidadãos a qual não tem regulamentação específica e o quanto esta sendo prejudicial para a população esse uso desmedido:

> Tem sido aplicado de forma totalmente desregulada. Não há regulação específica para utilização do reconhecimento facial na segurança pública no Brasil. Inclusive, a Lei Geral de Proteção de Dados (LGPD) não abarca essa utilização, porque no artigo 4º a lei determina que a segurança pública e a defesa nacional não estão no escopo das determinações colocadas no texto. Então, temos um cenário de completa desregulação, aliado a um crescente aumento de projetos sendo desenvolvidos por polícias e guardas municipais por todo o território nacional.
> É um cenário que é um complicador, porque a gente não encontra uma base mínima para que esse tipo de tecnologia pudesse ser utilizado. Ou seja, protocolos operacionais, regulação, determinações claras de quem, quando e como será feito o acesso aos dados das pessoas, o ciclo de vida desses dados, quem vai ser responsável pelos erros ocorridos durante essa implementação. A gente não tem esse estudo básico para ter o início desses projetos.
> [...]
> O que a gente encontrou aqui no Rio de Janeiro foi o relatório de utilização das câmeras em um dia, nos arredores do Maracanã, demonstrando que 63% das pessoas que foram detidas naquele dia foram detidas erroneamente, não eram pessoas que tinham mandados de prisão expedidos em seu nome. Então, o que a gente tem visto é exatamente uma falta de atenção e de regulação do uso dessas tecnologias. Sabemos que as tecnologias de reconhecimento facial produzem muito mais danos do que avanços, do que elementos positivos para garantia de direitos, para melhora na gestão das agências de segurança. Então, nossa posição é pelo banimento.(Soares, 2022)

Por outro lado, conforme ressalta o prefeito Ricardo Nunes, ao comentar que o sistema Smart Sampa alcançou o auxílio na captura de mais de 1.000 foragidos em 6 meses:

> O número de prisões de foragidos pelo Smart Sampa reforça a certeza de uma cidade mais segura. Cada criminoso preso, após identificação pelas câmeras de reconhecimento facial, significa que evitamos muitos crimes. Para o cidadão de bem fica a mensagem: Sorria, você está sendo protegido. (Smart Sampa, 2025)

Assim, encontramo-nos em um momento de dilema entre a eficiência do maior sistema de monitoramento do país e a ineficácia da regulamentação existente.

4.2 O tratamento com as informações pessoais nas cidades inteligentes

As cidades inteligentes, não são somente o espaço urbano territorial, elas acontecem principalmente no novo ambiente, denominado ciberespaço, o qual tem como definição pelas normas que definem cidades inteligentes:

> [...] são cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação. (Carta Brasileira para Cidades Inteligentes, 2022).

Logo, como no espaço terrestre, esse novo ambiente é vulnerável para ataques, e o Guia de Cibersegurança para Cidades Inteligentes desenvolvido pelo Banco Interamericano de Desenvolvimento (BID), publicado em dezembro de 2021, cita os principais tipos de ataque:

> Os alvos de um ataque cibernético podem ser informações, hardware, software , serviços oferecidos, redes e conexões, recursos humanos, infraestrutura cibernética crítica e, em geral, qualquer bem ou serviço municipal que utilize TICs. Os ataques mais frequentes estão relacionados ao uso de engenharia social, programas mal- intencionados, força bruta para obter acesso e ataques a conexões e infraestrutura. Tais ações visam, entre outros objetivos, atentar contra a privacidade, integridade ou disponibilidade dos sistemas de informação e, de forma geral, driblar medidas de segurança (Hueso; Acevedo, 2021, p. 38)

Em razão disso, as cidades inteligentes necessitam de segurança, e esta foi intitulada de cibersegurança, cuja definição se deu pela União Internacional de Telecomunicações:

> Conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de riscos, ações, capacitação, melhores práticas, seguros e tecnologias que podem ser usados para proteger os ativos da organização e os usuários no ambiente cibernético.

> Os ativos da organização e dos usuários são os dispositivos de computação conectados, o pessoal, os serviços/aplicativos, os sistemas de comunicação, as comunicações multimídia e todas as informações transmitidas e/ou armazenadas no ambiente digital.
> A cibersegurança garante a aplicação e manutenção das propriedades de segurança dos ativos e usuários da organização contra os respectivos riscos de segurança no ambiente cibernético. (UIT, 2018)

Ademais, a cibersegurança exerce a função de afrontar os riscos pertinentes aos serviços prestados no espaço digital. A Organização para a Cooperação e Desenvolvimento Econômico descreveu as dimensões, as quais ela irá proteger:

> 1) a tecnologia, quando incide no funcionamento do ambiente digital (muitas vezes chamada pelos especialistas de “segurança da informação”, “segurança de TI” ou “segurança da rede”); 2) a aplicação da lei ou aspectos jurídicos (por exemplo, crimes cibernéticos); 3) a segurança nacional e a estabilidade internacional, inclusive aspectos como o papel das TICs na inteligência, prevenção de conflitos, guerra, defesa cibernética, etc., e 4) a dimensão econômica e social , que compreende a criação de riqueza, inovação, crescimento, competitividade e emprego em todos os setores econômicos, liberdades individuais, saúde, educação, cultura, participação democrática, ciência, lazer e outras dimensões do bem-estar em que o ambiente digital promove o progresso. (OCDE, 2015)

Dessa forma, no Brasil atualmente a cibersegurançase manifesta por meio da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), a qual é uma legislação protetiva aos dados pessoais. Entretanto, essa legislação não trata especificamente dos dados nas smartcities mas tutela sobre essas informações em ambientes variados.

Vargas destaca três grandes eixos para agregar a proteção de dados pessoais com a expansão das cidades inteligentes:

> (i) a compreensão de que se está diante de grande espectro conceitual, tendo em vista que a União Internacional de Telecomunicações - UIT aponta, pelo menos, 116 definições conceituais para a expressão "cidade inteligente"; (ii) a compreensão dos limites e desafios do estado da arte da governança digital no Brasil (embora, nesse ponto, a recentíssima lei Federal 14.129, de 29 de março de 2021 sinalize desejável mudança); (iii) a compreensão ampliativa da tônica das atividades de tratamento de dados, e sua imperiosa proteção, quando realizada pelo Poder Público. (Vargas, 2021)

Assim, neste contexto de cidades inteligentes, há esse destaque para a dimensão coletiva da proteção de dados, então segundo os autores Danilo Doneda e Diego Machado, ao usar a técnica de profiling automatizado o qual irá prever o comportamento de determinadas coletividades, cujo método é adverso ao art 5º, inciso I da LGPD que determina a perspectiva tradicionalmente da tutela individual da privacidade e do conceito de dados pessoais.

Em razão disso, os autores determinam um rol de relações jurídicas, o qual os sistemas

implementados em cidades inteligentes deveriam ser constituídos, como:

> a) Direito ao anonimato ou anonimização de dados: a informação pessoal coletada em sistemas de cidades inteligentes deverá ser objeto de tratamento somente se necessária e adequada à finalidade de sua coleta e processamento, do contrário, se excessiva, deve ser anonimizada, conforme a Lei Geral de Proteção de Dados (LGPD), art. 6º, III;
> b) Direito à revisão de decisão tomada por sistemas automatizados que proporcionem ilegítima interferência em interesses juridicamente protegidos do titular dos dados (LGPD, art. 20);
> c) Obrigação de adotar as pertinentes medidas técnicas e administrativas de segurança (arts. 6º, VII, 46), de modo a implementar padrões de segurança informacional confiáveis de acordo com o estado da arte;
> d) Encargo de realizar relatórios de impacto à proteção de dados pessoais (RIPD).

Outro meio de proteção dos dados coletados pelas redes do governo e sua divulgação, eles são resguardados pelas políticas de regulamentação do acesso a informação no Brasil, por meio da Lei de Acesso à Informação (Lei 12.527/2011), em seu art 3º:

> Art 3º [...]
> I – conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
> II – possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
> III – possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina.

Ademais, desenvolvida pelo Ministério do Desenvolvimento Regional, com iniciativa filiada à Política Nacional de Desenvolvimento Urbano (PNDU), entre outras colaborações, foi redigida a Carta Brasileira para Cidades Inteligentes, a qual tem como objetivo ser uma estratégia nacional para cidades inteligentes. Dentre os objetivos estratégicos determinados por essa agenda brasileira para cidades inteligentes, está o de estabelecer um sistema de governança de dados:

> 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. (Carta brasileira para cidades inteligentes, 2022, p. 33 e 34)

Diante deste objetivo estratégico, a agenda brasileira para cidades inteligentes determina que seria possível assegurar a segurança dos dados compartilhados e a proteção jurídicados cidadãos.

As empresas de TICs devem manter a transparência de seus dados e softwares de códigos abertos ou livre. O mais importante, é que suas diretrizes estejam alinhadas com o Sistema Nacional para Transformação Digital. O documento nacional menciona sobre o uso da Política de Dados Abertos, defendendo que dados governamentais devem estar disponíveis para qualquer pessoa com uma possibilidade de redistribuição em qualquer forma, sem qualquer restrição de direitos autorais. Assim, ocorrerá a facilidade de acessar e compartilhar os dados governamentais, mas esse acesso haver rigorosos critérios de segurança para com essas informações, devido a ética em sua utilização e observar a proteção a privacidade individual.

Desta forma, além de aplicar no administrativo, outra recomendação seria na aplicação dessa política nos dados geoespaciais e meios imobiliários, afim de otimizar os sistemas para que trabalhem juntos e uniformizar vocabulários, métodos, dentre outros. E por fim, a última recomendação refere-se as plataformas públicas de compartilhamento de dados, as quais devem ser inclusivas, georreferenciadas, e determina quatro objetivos para essas plataformas, o que leva à sua anonimização, assim como, avaliar a necessidade da coleta de alguns dados e o plano das políticas de uso.

CONSIDERAÇÕES FINAIS

Este trabalho possui como objetivo explorar o conceito de cidades inteligentes, sua aplicação prática e aprofundar sobre o direito á privacidade e sua relação com este novo projeto de organização urbana.

Os dados adquiridos pelo uso de diferentes meios tecnológicos para monitorar e registrar todos os movimentos do espaço urbano são armazenados, e seu acesso e controle é restrito aos gestores públicos. Por isso, ao utilizar indevidamente esses dados, como por exemplo, fornecer para empresas privadas, ou manipular de modo não transparente, poderá ocasionar em uma violação do direito a privacidade dos cidadãos, garantia esta constitucional.

Em razão disso, buscamos compreender a importância das cidades inteligentes em aplicar corretamente o direito à privacidade em relação aos dados pessoais coletados de seus

cidadãos, cumprindo com a Constituição Federal de 1988 e com a Lei Geral de Proteção de Dados, ao restringir e controlar o acesso a essas informações.

Ademais, foi realizado estudos sobre os conceitos dessa nova forma de organização urbana, as quais são ambientes tecnológicos que se utilizam de dados coletados da população para seu funcionamento.Além da realização de análises de como a administração pública, atualmente, está lidando com o desenvolvimento das cidades inteligentes paralelo a proteção das informações pessoais de seus cidadãos, afim de evitar seu vazamento ou venda para empresas.

Desse modo, concluiu-se ser necessário, para se evitar que indivíduos inocentes sejam prejudicados, o planejamento urbano junto das legislações como a aplicação da LGPD, do Marco Civil da Internet, da Lei de Acesso á Informação.

Ademais, outras formas de organizaçãoda cibersegurança nas smarties cites seriam normas locais quanto a regulamentação do tratamento de dados em serviços públicos, a interoperalidade entre sistemas.

Em relação as empresas privadas,seria recomendável diretrizes, normas e procedimentos para a infraestrutura de seus sistemas. E aos dados públicos, a possibilidade de aplicação da Declaração do Governo Aberto, cujo objetivo é facilitar o acesso aos dados governamentais, porém comacesso rigoroso em relação aos critérios de segurança.

Logo, existem diferentes fatores que contribuem para que a coleta de informações pessoais seja tratada de forma adequada para assim as cidades inteligentes serem implementadas de forma assertivas.

REFERÊNCIAS

ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. *Planejamento urbano do futuro, dados do presente***:** a proteção da pivacidade no contexto das cidades inteligentes. Revista brasileira de estudos urbanos e regionais, v.22, e202003, 2020. Disponível em: https://doi.org/10.22296/2317-1529.rbeur.202003. Acesso em 15 nov. 2024

BECK, Ulrich. *Sociedade de Risco – Rumo a uma outra modernidade*. São Paulo: Editora 34, 2013.

BRASIL. Ministério do Desenvolvimento Regional (MDR) ... [et al]. *Carta Brasileira para Cidades Inteligentes*. 1. Ed. 2020. Disponível em: https://internetlab.org.br/wpcontent/uploads/2021/01/carta_brasileira_cidades_inteligentes.pdf. Acesso em: 15 nov. 2024

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Relatório do MCTI aponta que indústria de Software e Serviços de TIC cresceu 6,5% no Brasil em 2021*. Site Gov.br. Jul. 2022. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2022/07/relatorio-do-mcti-aponta-que-industria-de-software-e-servicos-de-tic-cresceu-6-5-no-brasil-em-2021. Acesso em: 15 nov. 2024.

CABRAL, Marcelo Malizia. *A colisão entre os direitos de personalidade e o direito de informação*. In: FRUET, Gustavo Bonato; MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz (Org.). Direitos da personalidade. São Paulo: Atlas, 2012. p. 108-152.

CASTELLS, Manuel. *A Sociedade em Rede - A era da informação, economia, sociedade e cultura*. São Paulo: Paz e Terra, 1999. v.1.

COLOMBO, Cristiano. BERNI Duílio Landell de Moura. *Privacy no Direito Italiano: Tríade de Decisões Judiciais rumo a Insights sobre Limites Conceituais, Deslocamento Geográfico e Transparência do Corpo Eletrônico*. Revista IBERC. v. 5, n. 1, p. 112-131, jan./abr. 2022. https://doi.org/10.37963/iberc.v3i2.205

DAMO, Paola Salvatori. *Pandemia do novo coronavírus à luz da Lei Geral de Proteção de Dados*. Migalhas, 14 abr. 2020. Disponível em: https://www.migalhas.com.br/depeso/324507/pandemia-do-novo-coronavirus-a-luz-da-lei- geral-de-protecao-de-dados. Acesso em: 12 abr. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2021.

DONEDA, Danilo; MACHADO, Diego. *Cidades Inteligentes, Dados Pessoais e Direitos Dos Cidadãos no Brasil*. Site CyberBRICS. Mai. 2019. Disponível em: https://cyberbrics.info/cidades-inteligentes-dados-pessoais-e-direitos-dos-cidadaos-no-brasil/ Acesso em: 15 nov. 2024

ESTADÃO CONTEÚDO. *TIM fecha parceria com Prefeitura do Rio para rastrear movimento e combater vírus*. InfoMoney, 23 mar. 2020. Disponível em: https://www.infomoney.com.br/economia/tim-fecha-parceria-com-prefeitura-do-rio-para-rastrear-movimento-e-combater-virus/. Acesso em: 12 abr. 2025.

FERRAZ JUNIOR, Tércio Sampaio. *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito,* Universidade de São Paulo, 8.ed, 1993.

HUESO, Lorenzo Cotino. ACEVEDO, Marco Sánchez. *Guia de cibersegurança para cidades inteligentes*. 2021. https://doi.org/10.18235/0003876.

LEMOS, André. *Cidades Inteligentes: Lugar, Territorialização Informacional e Inteligência*. Disponível em http://www.lab404.ufba.br/?p=2491. Acesso em 01 nov 2024.

MONTEFUSCO, Renato Zanolla. SOUSA, Cidoval Morais de. GIOLO JUNIOR Cildo. MARTOS, Frederico Thales de Araújo. *Smart Cities: Sandbox Epistêmico para uma Economia Circular Restaurativa e Regenerativa*. Revista Aracê. 2024. DOI: https://doi.org/10.56238/arev7n1-195.

OCDE (Organización para la Cooperación e el Desarrollo Económicos). 2015. *Digital Security Risk Management for Economic and Social Prosperity*: OECD Recommendation and Companion Document. París: OCDE. Disponível em: <http://dx.doi.org/10.1787/9789264245471- en> Acesso em: 15 nov. 2024

RIOS NETO, João Vieira; GIMENEZ, Edson Josias C. ***Cidades Inteligentes: sua contribuição para o desenvolvimento urbano sustentável***. **VII SRST – Seminario de Redes e Sistemas de Telecomunicações Intituto Nacional de Telecomunicações – INATEL.** Set. 2018.

SÃO PAULO. *PL 385, de 23 de junho de 2022*. Diário Oficial, São Paulo, 2022. Disponível em: https://www.al.sp.gov.br/propositura/?id=1000448817. Acesso em: 15 nov. 2024.

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

2007.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Sanilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar , 2008.
SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas , 2013.

SMART SAMPA alcança a marca de 1.000 foragidos da Justiça capturados em 6 meses. *Revista Segurança Eletrônica*, São Paulo, 22 abr. 2025. Disponível em: https://revistasegurancaeletronica.com.br/smart-sampa-alcanca-a-marca-de-1-000-foragidos-da-justica-capturados-em-6-meses/. Acesso em: 22 abr. 2025.

SOARES, Nicolau. *Reconhecimento facial na segurança pública é "nova aposta no encarceramento", diz especialista*. Brasil de Fato, São Paulo, 29 jun. 2022. Disponível em: https://www.brasildefato.com.br/2022/06/29/reconhecimento-facial-na-seguranca-publica-e nova-aposta-no-encarceramento-diz-especialista/. Acesso em: 12 abr. 2025.

SOLOVE, Daniel J., *Understanding privacy*. Cambridge: Harvard University Press, 2008.

SUPREMO TRIBUNAL FEDERAL. *STF suspende compartilhamento de dados de usuários de telefônicas com IBGE*. Notícias STF, 7 maio 2020. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902. Acesso em: 12 abr. 2025.

UIT (União Internacional de Telecomunicações). 2008. *Cláusula 3.2.5 de la Rec.* UIT-T X.1205 (04/2008). Genebra: UIT. Disponível em: <https://handle.itu.int/11.1002/1000/9136>. Acesso em: 15 nov. 2024

UNITES STATES. Library of Congress. *Olmstead v. United States, 277 U.S. 438, 478 (1928).* Brandeis, J., dissenting. Disponível em: https://www.loc.gov/item/usrep277438/. Acesso em 20/04/2025.

VAN DIJK Jan A.G.M. *The Network Society.* 2.ed. London: SAGE, 2006.

VARGAS, Isadora Formenton. *Três fundamentos à cidade inteligente*: a tônica da proteção de dados no Poder Público. In: CRAVO, Daniela Copetti; CUNHA, Daniela Zago Gonçalves da; RAMOS, Rafael (Coord.). Lei Geral de Proteção de Dados e o Poder Público. Porto Alegre: Centro de Estudos da PGM/Escola do Tribunal de Contas do Estado do Rio Grande do Sul, 2021. No prelo. Disponível em: < https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342754/cidades-inteligentes-smart-cities-e-protecao-de-dados-pessoais> Acesso em: 15 nov. 2024

WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. *Harvard Law Review*, v IV, n 5, December, 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 15 nov. 2024

WEISS, Marcos Cesar. BERNARDES, Roberto Carlos. CONSONI, Flavia Luciane. *Cidades inteligentes como nova prática para o gerenciamento dos serviços e infraestruturas urbanos*: a Experiência da Cidade de Porto Alegre. Revista Brasileira de Gestão Urbana (Brazilian Journal of Urban Management), 2015 set./dez., 7(3), 310-324.