JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1
FLUXO CONTÍNUO – ANO 2023 - MÊS DE NOVEMBRO – ED. 47. Vol. 1. Págs. 458-474

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

Facit.TO
FACULDADE DE CIÊNCIAS DO TOCANTINS

AS CIDADES INTELIGENTES (SMART CITIES) À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

SMART CITIES IN LIGHT OF THE GENERAL DATA PROTECTION LAW

Cinthia Gonçalves SOARES
Centro Universitário Presidente Antônio Carlos (UNITPAC)
E-mail: cinthiagsoares98@gmail.com
ORCID: http://orcid.org/0009-0005-7274-0221

Lorena Sousa Bezerra AQUINO
Centro Universitário Presidente Antônio (UNITPAC)
E-mail: lorena10bezerra@hotmail.com
ORCID: http://orcid.org/0009-0001-8056-8397

Taciana Pita NUNES
Centro Universitário Presidente Antônio (UNITPAC)
E-mail: taciana.pita@gmail.com
ORCID: http://orcid.org/0009-0007-4302-0465

RESUMO

As chamadas Cidades Inteligentes (smarts cities) trazem a ideia de acessibilidade aliada à segurança dos usuários inseridos nessa esfera. Entretanto, essa inovação tecnológica pode acarretar em riscos potenciais quanto à coleta de dados pessoais e sensíveis, uma vez que é fundamental equilibrar os benefícios desta tecnologia com a proteção da privacidade dos cidadãos. Por isso, discutir esta lacuna que está em evidência nesse novo conceito de sociedade, promove um olhar crítico sob a falsa ideia de liberdade e privacidade, aliada ao discurso de evolução das sociedades. O presente estudo visa analisar as consequências advindas do avanço tecnológico que trouxe esse novo conceito de desenvolvimento nos âmbitos da conjuntura social, com o intuito de alcançar uma melhoria na governança da população. Diante disso, busca-se analisar o desenvolvimento das smarts cities à luz da Lei Geral de Proteção de Dados, especialmente no que se refere aos princípios da finalidade, transparência e segurança, e como o ordenamento jurídico acompanha as mudanças resultantes dessa inovação.

Palavras-chave: Cidades Inteligentes. Dados pessoais. LGPD. Princípios.

ABSTRACT

The so-called Smart Cities bring the idea of accessibility combined with the safety of users within this sphere. However, this technological innovation can lead to potential risks regarding the collection of personal and sensitive data, as it is essential to balance the benefits of this technology with the protection of citizensprivacy. Therefore, discussing this gap that is in evidence in this new concept of society, promotes a critical look under the false idea of freedom and privacy, combined with the discourse on the evolution of societies. The present study aims to analyze the consequences arising from the technological advances that have brought this new concept of development within the social context, with the aim of achieving an improvement in the governance of the population. In view of this, we seek to analyze the development of smart cities in light of the General Data Protection Law, especially with regard to the principles of purpose, transparency and security, and how the legal system follows the changes resulting from this innovation.

Keywords: Smart cities. Personal data. LGPD. Principles.

INTRODUÇÃO

Na atual conjuntura social onde a "revolução algorítmica" é constante, fica evidente cada vez mais a falsa ideia de independência, segurança e liberdade à luz das necessidades dos indivíduos inseridos nesse contexto.

Seguindo essa linha de raciocínio, as Cidades Inteligentes (Smart Cities) são exemplos de espaços que utilizam de recursos tecnológicos que objetivam garantir uma maior qualidade de vida ao cidadão, de forma a proporcionar a eles segurança, sustentabilidade, desburocratização de serviços e entre outros benefícios.

Na realidade, contudo, tais cidades coletam dados pessoais e sensíveis da população em alta escala, o que levanta o questionamento sobre o modo de armazenamento e tratamento desses dados, e ainda acerca dos riscos de vazamento, e, sobretudo, de um controle exacerbado do Estado, com o discurso da garantia de segurança.

Sob esse viés, diante da crescente proliferação de dados coletados e processados por meio da inteligência artificial, expõem-se a problemática acerca do direito à privacidade e demais riscos diante do controle sobre essas informações, de onde surgem indagações do tipo: Quanto mais segurança, menos privacidade? Quanto maior o controle, menor a liberdade?

Partindo desse pressuposto, constata-se que a retenção de dados pessoais e sensíveis pode ficar sob uma vertente de controle social prematura, visto que apresentam lacunas no que diz respeito à governança dos dados coletados pelos serviços oferecidos.

Nesse sentido, o presente estudo pretende esclarecer o contexto em que surgiram as cidades inteligentes, apresentando uma breve análise à luz da Lei Geral De Proteção de Dados.

Para tanto, o desenvolvimento deste trabalho adotou pesquisa bibliográfica básica, utilizando artigos científicos, obras literárias e documentos legislativos pertinentes ao assunto, apresentando cunho qualitativo e exploratório a qual investigará acerca da temática de modo a possibilitar maior conhecimento sobre as questões abordadas.

Objetivo preponderante é analisar a efetividade da garantia do direito à privacidade e à liberdade no funcionamento das cidades inteligentes, sob a ótica da Lei Geral de Proteção de Dados-LGPD, especialmente em relação aos princípios da finalidade, transparência e segurança. De forma mais específica, pretende-se compreender o funcionamento das cidades inteligentes e as modificações que trarão para o sistema social, evidenciar o risco de violação dos direitos personalíssimos do indivíduo no que diz respeito a coleta massiva dos dados pessoais e sensíveis e explorar a relevância da aplicação da Lei Geral de Proteção de Dados no desenvolvimento das cidades inteligentes.

Para tanto, ao longo do segundo capítulo abordou-se sobre o conceito de smart cities e o seu objetivo principal no que tange ao desenvolvimento dos espaços urbanos, elucidando também como esse novo ideal começou a ser discutido a fim de promover uma interseção entre os eixos urbanístico, tecnológico e da arquitetura como forma de facilitar o cotidiano nas cidades por meio dos dados dos cidadãos que as compõem.

O terceiro capítulo apresenta sobre os direitos da personalidade e como eles são percebidos no tratamento de dados das cidades inteligentes. A partir disso a análise desse novo conceito de sociedade demonstra que este necessita acompanhar a previsão legal da Carta Magna, que visa garantir os direitos basilares como a proteção à imagem, nome, liberdade e privacidade dos cidadãos, elucidados também no Código Civil com o tema direitos da personalidade, de modo a assegurar os direitos inerentes à pessoa humana.

E, por fim, no quarto e quinto capítulos discute-se sobre a regulamentação da LGPD (Lei Geral de Proteção de Dados) frente ao desenvolvimento das cidades inteligentes, quais seriam os pilares na orientação no que tange ao tratamento dos dados pessoais, de forma a garantir a privacidade, transparência e segurança dos indivíduos inseridos nesse novo contexto tecnológico.

NOÇÕES GERAIS ACERCA DAS CIDADE INTELIGENTES

Por cidade inteligente entende-se como uma abordagem inovadora que incorpora desenvolvimento urbano com a utilização de dados dos cidadãos que compõem uma conjuntura social, objetivando principalmente melhorar a qualidade de vida destes indivíduos.

Sob a ótica de André Lemos "as cidades inteligentes são compostas por processos sensíveis ao contexto, lidando com um gigantesco volume de dados, redes em nuvem e comunicação entre diversos objetos" (Lemos, p.48, 2013).

Partindo desse entendimento, pode-se compreender tais unidades, como espaços urbanos que tem como objetivo ampliar a eficiência das cidades em seus aspectos político- econômico e social, com o fito de promover a melhor qualidade de vida de seus habitantes.

Dessa forma, o despertar para o surgimento das Cidades Inteligentes (smart cities) se deu na década de 1990, e o conceito começou a ser discutido por diversos autores, sendo um dos pioneiros o escritor William J. Mitchell, autor do livro "City of Bits: Space, Place, and the Infobahn"[1] (1995) que trouxe a associação de três eixos, a tecnologia da informação, urbanismo e a arquitetura.

A obra enfatiza a exploração dessas três interseções, visando que o ambiente urbano se tornasse mais eficiente, acessível e habitável, para acompanhar o avanço

tecnológico a partir de novas políticas de planejamento urbano de forma a promover serviços focados na gestão e melhoria da infraestrutura urbana.

Posto isto, constata-se que essas cidades são uma inovação que se baseia no aprimoramento dos recursos para a gestão da vida em comunidade, com pilares de sustentabilidade e desenvolvimento tecnológico.

Neste diapasão, tais cidades se materializam através de uma estrutura baseada em inteligências artificiais[2] que guiaram o desenvolvimento de empresas e o cotidiano dos cidadãos. (DEPINE, 2016).

De acordo com o estudo The World Population Prospects: The 2017 Revision (2017)[3] [1], a população mundial chegará a 8,6 bilhões em 2030, com isso a aplicação das smart cities propiciará benefícios no que se refere à facilitação da mobilidade e transporte, melhoramento econômico, sustentabilidade ambiental, entre outras bases de desenvolvimento.

No entanto, para a eficiência dessas cidades, é necessário o recolhimento de dados pessoais e sensíveis da sociedade, de forma a mapear e gravar o cotidiano dos habitantes, provocando a evidência de um sistema que promete ser mais seguro no que concerne a análise minuciosa das necessidades dos cidadãos visando o aprimoramento dos serviços públicos, mas, em contrapartida, invasivo, uma vez que o Estado terá em suas mãos informações sensíveis, passando a população a viver em estado de constante vigilância, e, porque não, em estado constante de violação dos direitos da personalidade?

Sob esse viés, é relevante discutir sobre os desafios encontrados na perspectiva da governança dos dados e como são geridos tais elementos pessoais coletados e armazenados, visto que esse campo de segurança e ecossistema de pessoas, processos e tecnologias pode evidenciar uma lacuna de exploração de vulnerabilidades que podem causar um alerta no que se refere às cidades inteligentes. (PUSCHI; SILVA; SANTOS, 2022).

---

[1] [1] “Cidade dos Bits: Espaço, Lugar e Infobahn” (1995)

[2] As primeiras discussões sobre o termo “inteligência artificial” surgiu em 1955 por meio do matemático John McCarthy, sendo este conceito definido como campo da ciência da computação que busca por meio de sistemas e algoritmos realizar atividades diversas que objetivam simular as funçes cognitivas humanas
(KAUFMAN, 2019).

[3] As Perspectivas da População Mundial: A Revisão de 2017 (2017)

A partir da compreensão da delicadeza que é coletar e armazenar dados pessoais e sensíveis de milhares de pessoas, se faz necessário refletir acerca de como e onde serão armazenados, e ainda mais sob a responsabilidade pelo tratamento desses dados, de modo a garantir os direitos constitucionais fundamentais dos cidadãos, especialmente a privacidade e liberdade.

Um fato histórico importante e que merece destaque no contexto da presente abordagem teórica, ocorreu durante o governo Nazista de Adolf Hitler. O livro "IBM e o Holocausto" de Edwin Black (2001), relata que a empresa Internacional Business Machiness – IBM - por meio de uma tecnologia avançada para a época, colaborou decisivamente para o cometimento das atrocidades do governo de Hitler, ao coletar e entregar ao governo informações pessoais dos indivíduos, de modo a identificá-los - se tratava de judeus, ciganos ou outros considerados aptos para serem levados ao campo de concentração.

Assim, a partir do exemplo mencionado, a coleta de dados pessoais pode abrir precedentes inimagináveis, a depender do momento histórico que a sociedade atravessa, e a forma como são tratados.

Infere-se, portanto, que as cidades inteligentes garantem um desenvolvimento eficiente em diversos âmbitos da construção de uma sociedade, garantindo facilidade ao cotidiano dos indivíduos inseridos nessa esfera, contudo, é preciso desenvolver meio de alerta e cuidado ao implementar tal sistema, visando evitar interferências na vida privada e na liberdade dos indivíduos, e até mesmo não ser caminho para um novo holocausto - o que pode soar impossível, no entanto, a guerra entre Israel e Hamas (Palestina), mostra que a história pode sim se repetir.

DIREITOS DA PERSONALIDADE NO TRATAMENTO DE DADOS COLETADOS PELAS CIDADES INTELIGENTES

No limiar do século XXI, observa-se que o avanço no âmbito tecnológico permite aos usuários inseridos nessa esfera uma interação com o mundo de forma inteligente, de modo a possibilitar a captação de informações e a transmissão dos dados pessoais e sensíveis dos indivíduos. Nesse sentido, mesmo que tais mecanismos revelem um lado positivo quanto a agilidade e praticidade no cotidiano de quem utiliza essas ferramentas tecnológicas, estes podem apresentar lacunas que provocam uma

exposição dos dados e informações coletadas dos usuários, de modo a violar os direitos da personalidade intrínsecos a eles.

Segundo Amaral (2017), os direitos da personalidade consistem no conjunto unitário, dinâmico e evolutivo dos bens e valores essenciais da pessoa no seu aspecto físico, moral e intelectual. Diante disso, tais direitos garantem a proteção à imagem, nome, liberdade e privacidade dos cidadãos, no que diz respeito aos direitos fundamentais elucidados na Constituição Federal de 1988

Assim, a proteção constitucional dos direitos fundamentais, no que tange especificamente o direito à privacidade, é protegido pelo inciso X do artigo 5º da Constituição, que assim dispõe: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". Importante ressaltar que este inciso faz conotação em sentido amplo, ao que se refere à proteção dos direitos íntimos, privados e da personalidade das pessoas.

Consoante a isso, constata-se que o desenvolvimento de Cidades Inteligentes pode provocar uma vulnerabilização dos direitos da personalidade resultando em danos irreversíveis para os indivíduos inseridos nesse contexto. Segundo o estudo da Surfshark (2022), empresa holandesa de segurança cibernética revela que o Brasil é o 12º país no ranking de vazamento de dados, o qual comprova os riscos existentes na governança e tratamento de dados coletados.

É válido ressaltar que a realidade do desenvolvimento das Cidades Inteligentes é bem próxima e que seu funcionamento depende do uso de inteligência artificial (IA), e que mesmo que possuam uma capacidade de beneficiar a vida dos indivíduos, estas poderão provocar dilemas no que tange ao direito à privacidade e à imagem da sociedade. O autor Kai-Fu Lee da obra "Inteligência Artificial" (2020), pondera que os usos destas ferramentas representam riscos promissores e perigos potenciais, de modo a modificar o funcionamento social.

Destarte, analisa-se que para a aplicação das smart cities é necessário observar as legislações existentes no que diz respeito aos direitos personalíssimos da pessoa humana, visto que o Código Civil de 2002 acentua que tais direitos são invioláveis, sendo caracterizados por este ordenamento jurídico como intransmissíveis e irrenunciáveis (BRASIL, 2002). Ademais, faz-se necessário também a utilização de

legislações específicas para regular a série de dados e informações que serão capturados, tratados e armazenados (PARINI; PEGORARO, 2021).

O tratamento do tema direitos da personalidade no Código Civil, está disciplinado nos artigos 11 ao 21. Dando ênfase ao artigo 11, que elucida em sua redação as características dos direitos da personalidade, onde afirma que: "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.".

Contudo, constata-se que a automatização de serviços na sociedade através do desenvolvimento tecnológico deve considerar alguns pontos que garantam o equilíbrio entre o uso de inteligências artificiais e a humanidade, de modo a assegurar os direitos inerentes à pessoa humana.

A LEI GERAL DE PROTEÇÃO DE DADOS COMO REGULAMENTO PARA O DESENVOLVIMENTO DAS CIDADES INTELIGENTES

A Lei Geral de Proteção de Dados prevista no dispositivo jurídico n. 13.709/2018, objetiva regulamentar questões referentes ao meio tecnológico, a fim de manusear juridicamente os dados pessoais e sensíveis dos usuários dessa esfera, conforme é vislumbrado em seu artigo 6º, inciso I (LGP, 2018).

Diante disso, a pesquisadora Regina Ruaro, que faz parte do grupo internacional de pesquisa Protección de Datos, Transparência y Acceso a la Información (2022), revela que tal regulamentação garante que as informações coletadas sejam tratadas de modo que preserve a confidencialidade dos indivíduos e, ainda, a proteção da privacidade dos mesmos, sobretudo, no mundo online.

Sob esse viés, percebe-se a necessidade de trazer tal tema para o conhecimento de seus usuários, de modo que tenham a preocupação e atenção na forma como suas informações pessoais estão sendo utilizadas e que ao serem repassadas, lhe seja informado o motivo de tais transferências, visando uma maior transparência e participação dos usuários na utilização de seus dados.

Partindo disso, é válido salientar que ao se tratar de uma realidade cada dia mais evidente, que são as cidades inteligentes, a Lei Geral de Proteção de Dados torna-se uma importante base de regulamentação para aplicação das smart cities visto que a coleta de dados que ocorre por parte dos sensores trazem uma falsa garantia de

anonimização dos dados, resultando em uma proteção prematura e frágil (RAMIRO; CÂMARA, 2017).

Nesse contexto, é relevante destacar que a referida legislação é fundamentada pelos princípios da finalidade, transparência e segurança, os quais orientam o tratamento de dados pessoais de forma segura. Sob esse prisma, é imprescindível que as Cidades Inteligentes se desenvolvam baseadas nestes princípios de modo a evidenciar aspectos acerca da captura e tratamento de dados por meio das inteligências artificiais.

A CLASSIFICAÇÃO DOS DADOS APRESENTADA PELA LEI GERAL DE PROTEÇÃO DE DADOS

Para dar seguimento a compreensão dos riscos apresentados nas smart cities, é fundamental a diferenciação nas ramificações existentes nos conceitos de dados e o perigo que seu manuseio inadequado representa nesse novo modelo de sociedade.

De acordo com Veiga e Rover (2004), é possível separar tal definição em duas categorias, sendo elas: dados públicos e privados. Os dados públicos se caracterizam por ser de conhecimento geral e seu acesso independe de restrições, sendo estes de propriedade comum. Já os dados privados referem-se a informações sensíveis e geralmente individuais que são sigilosas e pessoais.

No entanto, para além da classificação em dados públicos e privados, a Lei Geral de Proteção de Dados apresenta sua própria definição e classificação. O art 5°, incisos I e II, assim diz:

> I- dado pessoal: informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018)
> II- dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado à uma pessoa natural. (BRASIL, 2018).

Dado pessoal se refere a qualquer informação que possa ser usada para identificar uma pessoa específica. Isso inclui uma ampla variedade de informações, como nome, endereço, número de identificação, endereço de e-mail, número de telefone, data de nascimento, entre outros.

Já os dados pessoais sensíveis, também conhecidos como dados pessoais altamente sensíveis, são informações pessoais que, se mal utilizadas ou divulgadas, podem causar danos substanciais ou discriminação significativa para a pessoa à qual se referem. Esses dados incluem informações que revelam características pessoais especialmente delicadas, como origem racial ou étnica, crenças religiosas ou filosóficas, orientação sexual, opiniões políticas, filiação a sindicatos, informações de saúde, informações genéticas e informações biométricas, como impressões digitais ou características faciais.

Logo, ressalta-se que essas classificações evidenciam com clareza os tipos de dados que podem sofrer riscos com a sua utilização indevida e velada pelo Poder Estatal, pois ao se tratar de informações referentes à individualidade de cada cidadão como ideologia, religião e origem racial é iminente a possibilidade de controle e falta de segurança. Assim, "A proteção dos dados pessoais, públicos ou privados, sensíveis ou não, está diretamente relacionada à tutela da intimidade e da vida privada dos indivíduos" (RAMINELLI; RODEGHERI, 2016, p. 94).

Portanto, dispor de informações dos atos da vida pessoal do cidadão para o funcionamento das cidades inteligentes, com a ideia de promover a prestação de serviços eficientes, saúde e segurança pública aprimorados expõe, na verdade, o perigo que reside na falta de cuidado na proteção desses dados, o que pode levar à exposição indevida, discriminação e abuso.

PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS E SUA IMPORTÂNCIA

Os princípios elencados na LGPD, servem como diretrizes fundamentais que orientam o tratamento de dados pessoais e são essenciais para proteger a privacidade dos indivíduos, promover a transparência e a responsabilidade das organizações que coletam e processam esses dados.

Tais princípios estão elencados no artigo 6º da Lei nº 13.709/18, e atuam como norteadores no processo de aplicação e interpretação da lei ao tratamento de dados pessoais. Assim dispõe o art. 6º da LGPD:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos,específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitda e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V- qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas 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 difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X- responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Diante do exposto, nota-se que a garantia da proteção dos dados pessoais se dá por meio da observância e aplicação dos princípis taxados no artigo supracitado.

De acordo com Pinheiro (2021, pg.18), a regulamentação da proteção de dados pessoais tem como base normas principiológicas, posto isto, verifica-se a importância de analisar e adequar os princípios ao tratamento dos dados pessoais. Nas palavras da autora: “A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não é atendido.” (PINHEIRO, 2021, p.18).

Ademais, será explorado os principais princípios em consonância a aplicação n o tratamento de dados nas cidades inteligentes.

O Princípio da Finalidade Aplicado à Coleta de Dados

O princípio da finalidade surge no ordenamento jurídico brasileiro com intuito de ressaltar a necessidade de se evidenciar o objetivo da utilização dos dados pessoais e sensíveis, seja para propósitos legítimos, específicos e explícitos. Seu conceito encontra- se no artigo 6º, inciso I, assim dispõe "finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;". Ou seja, trata-se de um princípio que regula a finalidade do processamento do tratamento de dados, dando segurança para que os dados do titular não sejam secundarizados de forma ilegal.

A célebre obra "1984" de George Orwell (2009), narra acerca de um Estado autoritário regido através de vigilância por meio de "teletelas" que monitorava os cidadãos em seu cotidiano. Tal regime era justificado para fiscalização do comportamento dos cidadãos como forma de garantir a ordem da sociedade. Todavia, a destinação dessas informações coletadas eram veladas, intensificando a ideia de controle total do Estado sob a vida da população.

Nesse sentido, fica evidente que a observância de tal princípio surge como forma de assegurar os direitos individuais, bem como garantir o uso das informações coletadas para finalidades que não ultrapassem as previsões constitucionais e legais.

Além de ser necessário a proteção dos direitos à privacidade dos cidadãos, é imprescindível que sejam aplicados meios de se promover uma confiança da população acerca da adoção de tais tecnologias e seus fins específicos.

Evaristo e Cesar (2014) afirmam que ao se tratar de qualquer tecnologia, o controle ainda é algo a ser buscado, enfatizando ainda que cabe ao Direito, como ciência, o dever de regular. Ou seja, as discussões sobre o tema pretendem alcançar equilíbrio das tecnologias e do ordenamento que as regem (EVARISTO; CESAR, 2014, p. 2).

Partindo desse entendimento, é possível refletir que para a introdução das Cidades Inteligentes deve-se demonstrar aos cidadãos-usuários a finalidade da coleta de seus dados, para que estes tenham conhecimento dos fins específicos de modo a permitir o manuseio destes elementos e reduzir o risco de uso secundário. Caso

contrário, a ausência de conhecimento sobre os fins de destinação das informações dos indivíduos possibilitará ao Estado exercer um controle sobre eles para diversas finalidades não especificadas, conforme representado na referida obra literária.

Por tais razões, o princípio da finalidade pode ser considerado um grande aliado da sociedade, quanto à implementação das cidades inteligentes.

O Princípio da Transparência na Realização do Tratamento de Dados

O Princípio da Transparência pode ser entendido como normatização da garantia aos titulares, de informações claras, precisas e facilmente acessíveis, sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comerciais e industriais, como discorre o inciso VI, do artigo 6º, da LGPD. Assim, evidenciando garantir que o controle de dados ocorra de forma clara e transparente, de modo a evidenciar os atos que serão realizados ao se valer de tais informações dos usuários que foram submetidos ao sistema tecnológico.

Além disso, Pestana (2022) aduz que tal transparência tem como objetivo também mostrar os agentes que realizam o tratamento de dados, sendo eles o controlador e o operador.

Sob esse viés, analisa-se que a presença o princípio da transparência no desenvolvimento das cidades inteligentes é necessário, visto que se relaciona ao caráter democrático a qual os cidadãos obtêm o direito de receber informações de como o ente governamental dispõe dos seus dados (JÚNIOR, 2022).

O documentário Citizenfour (2015) dirigido por Laura Poitras, relata a história de Edward Snowden, um ex-analista da Agência de Segurança Nacional dos Estados Unidos (NSA) que resolve expor esquemas de espionagem realizado por este órgão através do monitoramento dos cidadãos com a justificativa de garantia de segurança aos indivíduos. Com isso, percebe-se as possíveis consequências da utilização de dados pessoais e sensíveis por governos e empresas privadas, sem que haja a devida transparência e seja esclarecida a destinação destas informações.

Desse modo, vislumbra-se que a necessidade da transparência no manuseio das informações, é um princípio norteador que deve acompanhar os sistemas inseridos na sociedade, bem como nas cidades inteligentes, onde os discursos de mais segurança,

mais tecnologia e mais desenvolvimento deve versar sobretudo, sob o entendimento da transparência, em todos os seus contextos.

Princípio da Segurança no Contexto das Cidades Inteligentes

O princípio da segurança refere-se à utilização de medidas 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 difusão, de acordo com o inciso VII, artigo 6º da LGPD.

Na obra de Edwin Black, chamada "IBM e o Holocausto", é possível perceber que a ausência de gestão com segurança dos dados pessoais serviu de base para o vazamento das informações das pessoas com a descodificação do cartão que trouxe ao governo nazista a facilidade na investigação das características da população.

Nesse sentido, com o aumento da tecnologia, em meados da década de 70, surge a necessidade de se gerir os dados pessoais que existia na União Europeia e assim, a OCDE - Organização para a Cooperação e Desenvolvimento Econômico (2022) registrou a s primeiras Diretrizes para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais.

A partir disso, pode-se perceber que o princípio da segurança surge como ponto relevante no que tange a assegurar a privacidade dos usuários. Tal pressuposto prima manter a seguridade no que se refere aos dados contidos na esfera tecnológica, para que estes não sejam vazados, bem como evite os riscos contidos nesse contexto, como o uso indevido das informações pessoais e demais consequências advindas dessa nova realidade.

Portanto, é de entendimento primário que a segurança deve ser o passo inicial na implementação de uma cidade inteligente, de modo a perceber os riscos que os dados pessoais dos seus usuários que estão submetidos nessa esfera possuem grande relevância para a própria ascensão do sistema.

CONSIDERAÇÕES FINAIS

Com o advento da tecnologia, aguçou-se o uso das ferramentas tecnológicas para obter e compartilhar informações, bem como a sua aplicação em diversas esferas

da sociedade, ao exemplo da segurança, infraestrutura e demais serviços oferecidos aos indivíduos.

Sob esse viés, infere-se que as cidades inteligentes representam uma grande revolução tecnológica e que podem contribuir em diversos âmbitos para a sociedade. Entretanto, observa-se que os pontos que envolvem toda a construção dessa nova realidade, podem acarretar a vulnerabilização dos direitos personalíssimos dos cidadãos, visto que promove a facilidade do vazamento dos dados sensíveis dos usuários desse novo contexto.

Dessa maneira, como todo viés de gestão social, a retenção de dados pessoais e sensíveis fica sob uma vertente de controle social prematura, de modo a evidenciar que as cidades inteligentes mesmo se intitulando como uma ferramenta de inteligência artificial que garante segurança e evolução, representa um risco potencial à sociedade de modo que vulnerabiliza o direito de privacidade e liberdade dos indivíduos.

Diante disso, compreende-se que para o desenvolvimento destas cidades é necessário observar as legislações existentes que versam acerca dos direitos fundamentais dos indivíduos, bem como, requer a existência de legislação específica para regular o tratamento de dados e informações recolhidos de forma massiva.

Nesse sentido, analisou-se o funcionamento das smarts cities sob a ótica da Lei Geral de Proteção de Dados, já que a mencionada lei visa assegurar o manuseio de dados pessoais e sensíveis dos usuários de forma segura e transparente. Com isso, verificou-se que tais cidades devem ser pautadas nos princípios da finalidade, transparência e segurança, de forma a garantir a governança dos dados de forma eficiente evitando que as informações dispostas ao Estado não sejam utilizadas para fins diversos que atingem diretamente os cidadãos/usuários em seus direitos fundamentais mais básicos, como liberdade e privacidade.

REFERÊNCIAS

AMARAL, Francisco. **Direito civil: introdução**. Saraiva Educação SA, 1998.

BLACK, E. **IBM e o Holocausto**. Rio: Editora Campus, 2001.

BRASIL. **Constituição** da República Federativa do Brasil, de 05.10.1988. Brasí´lia, 1988. Disponível em: <http://www.**planalto**.gov.br/ccivil_03/**Constituicao**/**Constituiçao**.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**.

CRUZ , Talita. **Cidades Inteligentes:** O que é Características, + Exemplos no Brasil. [S. l.], 2022. Disponível em: https://www.vivadecora.com.br/pro/cidades-inteligentes/. Acesso em: 9 out. 2022.

DEPINE' , Ágatha Cristine et al. **Fatores de atração e retenção da classe criativa: o potencial de Florianópolis como cidade humana inteligente**. 2016.

DOS SANTOS PUSCHI, Michele Lima; DA SILVA, Anderson Aparecido Alves; SANTOS, Alessandro S. Desafios de governança de sistemas de informações aplicados a centros de controle de cidades inteligentes. In: **Anais do III Workshop Brasileiro de Cidades Inteligentes.** SBC, 2022. p. 49-60.

JUNIOR, Paulo Henrique Silva Pereira et al. O documentário "citizenfour" em análise sob a ótica da transparência e da proteção de dados pessoais: insights na perspectiva da administração pública brasileira. **Perspectivas Contemporâneas**, v. 17, p. 1-13, 2022.

KAUFMAN, Dora. **A inteligência artificial irá suplantar a inteligência humana?**. ESTAÇÃO DAS LETRAS E CORES EDI, 2019.

LEE, Kai-Fu. **Inteligência artificial**. Globo Livros, 2019.

LEMOS, André. Cidades inteligentes. **GV-executivo**, v. 12, n. 2, p. 46-49, 2013

Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/**lei**/l14020.htm.

MAROSSI, Lucas. **Privacidade: Importância de dados pessoais sensíveis e a história por trás.** [*S. l.*], 2022. Disponível em: https://www.eteknovared.com.br/blog/privacidade-importancia-de-dados-pessoais- sensiveis-e-a-historia-por-tras/. Acesso em: 19 out. 2022.

PARINI, Francyelli; PEGORARO, Luiz Nunes. O Direito à privacidade e à imagem nas cidades inteligentes. **Revista da Faculdade de Direito da FMP**, v. 16, n. 2, p. 159-178, 2021.

PESTANA, Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). **São Paulo: revista Consultor Jurídico. Recuperado de https://www. conjur. com. br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd**, 2020

POITRAS, Laura. Citizenfour. **Lectures, publications reçues**, 2015.

ORWELL, George. **1984**. Editora Companhia das Letras, 2009.7

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. – 7. ed. – Barueri: Manole, 2015.

RAMIRO, Andre´; CA^ MARA, Ama´lia. A Privacidade Em Um Cenario Pansensitível De Internet Das Coisas & Cidades Inteligentes. **14 a 16 de Dezembro de 2017–Escola de Comunicações e Artes da Universidade de São Paulo.**, p. 358, 2017.

EVARISTO, Silvana Aparecida Cardoso; CESAR, Claudio Evaristo. **Direito x internet. In: Âmbito Jurídico, Rio Grande, XVII, n. 127, ago 2014**. Disponí´vel em: . Acesso em 23 setembro 2023.

RAMINELLI, Francieli Puntel; RODEGHERI, Letí´cia Bodanese. **A Proteção de Dados Pessoais na Internet no Brasil:** Ana´lise de deciso˜es proferidas pelo Supremo tribunal Federal. In: Revista Cadernos do Programa de Po´s-Graduaça˜o em Direito PPGDir./UFRGS. Disponí´vel em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936 Acesso em 23 setembro 2023.

ROVER, Aires Jose´. **Direito e Informática.** Sa˜o Paulo: Manole, 2004.

D'COSTA, A. Book in Focus: **City of Bits : Space, Place and the Infobahn by William J. Mitchell**. Disponí´vel em :<https://www.re-thinkingthefuture.com/rtf-architectural- reviews/a10473-book-in-focus-city-of-bits-space-place-and-the-infobahn-by-william-j- mitchell/>.

PINHEIRO, Patrí´cia P. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD)**. Sa˜o Jose´ dos Campos : Editora Saraiva, 2021. E-book. ISBN 9786555595123. Disponí´vel em: https://integrada.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 22 out. 2023.