UNIVERSIDADE FEDERAL DE MINAS GERAIS
Faculdade de Direito e Ciências do Estado
Programa de Pós-Graduação

Gabriel Ribeiro de Lima

CIDADE "INTELIGENTE" (*SMART CITY*): ENTRE O DIREITO URBANÍSTICO E A PROTEÇÃO DOS DADOS PESSOAIS

Belo Horizonte
2024

Gabriel Ribeiro de Lima

CIDADE "INTELIGENTE" (*SMART CITY*): ENTRE O DIREITO URBANÍSTICO E A PROTEÇÃO DOS DADOS PESSOAIS

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Mestre em Direito.

Área de pesquisa: Direito e Justiça.

Linha de pesquisa: Poder, cidadania e desenvolvimento no Estado Democrático de Direito.

Área de estudo: Direito, tecnologia e inovação.

Orientador: Prof. Dr. Leonardo Netto Parentoni

Coorientador: Prof. Dr. Guilherme Magalhães Martins

Belo Horizonte
2024

Ficha catalográfica elaborada pela bibliotecária Meire Queiroz - CRB-6/2233.

Lima, Gabriel Ribeiro de
L732c Cidade “inteligente” (*smart city*) [manuscrito]: entre o direito urbanístico e a proteção dos dados pessoais / Gabriel Ribeiro de Lima. - 2024.
163 f.: il.

Orientador: Leonardo Netto Parentoni.
Coorientador: Guilherme Magalhães Martins.
Dissertação (mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito.
Bibliografia: f. 150-163.

1. Tecnologia e direito - Teses. 2. Cidades inteligentes - Teses. 3. Proteção de dados - Teses. 4. Direito urbanístico - Teses. 5. Direito à privacidade - Teses. I. Parentoni, Leonardo Netto. II. Martins, Guilherme Magalhães. III. Universidade Federal de Minas Gerais - Faculdade de Direito. IV. Título.

CDU: 34:007

UNIVERSIDADE FEDERAL DE MINAS GERAIS

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

ATA DA DEFESA DA DISSERTAÇÃO DO ALUNO

GABRIEL RIBEIRO DE LIMA

Realizou-se, no dia 11 de março de 2024, às 14:30 horas, sala online, da Universidade Federal de Minas Gerais, a defesa de dissertação, intitulada *CIDADE "INTELIGENTE" (SMART CITY): ENTRE O DIREITO URBANÍSTICO E A PROTEÇÃO DOS DADOS PESSOAIS*, apresentada por GABRIEL RIBEIRO DE LIMA, número de registro 2022654310, graduado no curso de DIREITO, como requisito parcial para a obtenção do grau de Mestre em DIREITO, à seguinte Comissão Examinadora: Prof(a). Leonardo Netto Parentoni - Orientador (UFMG), Prof(a). Guilherme Magalhães Martins (Universidade Federal do Rio de Janeiro - UFRJ), Prof(a). Newton De Lucca (Universidade de São Paulo-USP), Prof(a). Eduardo Tomasevicius Filho (USP).

A Comissão considerou a dissertação:

(X) Aprovada, tendo obtido a nota 100 (cem).

( ) Reprovada

Finalizados os trabalhos, lavrei a presente ata que, lida e aprovada, vai assinada por mim e pelos membros da Comissão.
Belo Horizonte, 11 de março de 2024.

gov.br Documento assinado digitalmente
LEONARDO NETTO PARENTONI
Data: 11/03/2024 17:31:18-0300
Verifique em https://validar.iti.gov.br

Prof. Leonardo Netto Parentoni (Doutor) Nota: 100

gov.br Documento assinado digitalmente
GUILHERME MAGALHAES MARTINS
Data: 13/03/2024 22:41:50-0300
Verifique em https://validar.iti.gov.br

Prof. Guilherme Magalhães Martins (Doutor) Nota: 100

gov.br Documento assinado digitalmente
NEWTON DE LUCCA
Data: 12/03/2024 21:55:36-0300
Verifique em https://validar.iti.gov.br

Prof. Newton De Lucca (Doutor) Nota: 100

Prof. Eduardo Tomasevicius Filho (Doutor) Nota: 100

EDUARDO TOMASEVICIUS FILHO
Assinado de forma digital por EDUARDO TOMASEVICIUS FILHO
Dados: 2024.03.12 13:17:10 -03'00'

AGRADECIMENTOS

Agradeço a Deus por ter me dado condições para a realização deste trabalho. Foram dedicadas muitas horas de pesquisa e de escrita, das quais recebi imensa e indispensável ajuda divina.

Este trabalho também contou com a colaboração de muitas pessoas, a quem sou eternamente grato. Inicialmente, destaco minha esposa, *Ana Carolina Saraiva Cardoso*, companheira de todas as horas, que me apoiou incondicionalmente durante todo o processo e que é o amor da minha vida.

Agradeço aos meus pais, *Carlos Eduardo Corrêa de Lima* e *Déborah Macedo Ribeiro de Lima*, que sempre estiveram ao meu lado e são de imensurável importância para a minha vida. Sou eternamente grato por todo o esforço dispendido para a minha criação.

Também agradeço à minha irmã, *Bárbara Ribeiro de Lima*, que sempre torceu pelo meu sucesso, e meus avôs, *Afonso de Araújo Ribeiro* e *Geraldo Ferreira Lima*, grandes exemplos de profissionais e de pais. Faço menção às minhas amadas e saudosas avós, *Santuza Corrêa de Lima e Maria José de Macedo Ribeiro*, que estão comemorando, lá do céu, a conclusão dessa obra.

Agradeço aos meus queridos amigos e mentores, *Anilton Maia de Carvalho* e *Cari Campos Cravo,* que contribuíram ativamente para a minha formação pessoal.

Um agradecimento especial ao meu Orientador *Dr. Leonardo Netto Parentoni*, cujos ensinamentos ultrapassaram as barreiras do Direito e da Tecnologia, transformando-me em uma pessoa melhor. Agradeço também ao meu Coorientador *Dr. Guilherme Magalhães Martins*, pelas valiosas orientações e pelos excelentes materiais, ambos fundamentais para a confecção desta dissertação.

Aos amigos e colegas *José Luiz de Moura Faleiros Junior*, *Tales Calaza* e *Julia Lio Rocha Camargo*, agradeço pelas várias e importantes colaborações durante todo o meu percurso no Mestrado na UFMG, bem como pelos ótimos momentos que passamos juntos, dentro e fora do ambiente acadêmico.

Agradeço aos colegas e professores da *Faculdade de Direito da Universidade Federal de Minas Gerais (UFM*G), que me acolheram e me proporcionaram excelentes experiências. Estendo os meus agradecimentos aos colegas do Centro de Pesquisa em Direito, Tecnologia e Inovação (Centro DTIBR), fundamentais para o meu desenvolvimento acadêmico e profissional.

RESUMO

A implantação da tecnologia *smart city* nas cidades estrangeiras está promovendo a coleta e o processamento de dados pessoais em grande escala. Isto gerou uma preocupação global sobre os riscos de violação a direitos e garantias dos sistemas de proteção de dados pessoais no ambiente urbano.

Algumas cidades brasileiras estão em fase inicial de uso da *smart city*, o que evidencia a urgência do estudo jurídico sobre a proteção dos dados pessoais neste ambiente. Portanto, o problema deste trabalho é investigar as peculiaridades da proteção dos dados pessoais na implantação de *smart city*, identificando desafios e buscando apresentar medidas para lidar com essas questões no Brasil.

Para tanto, foram utilizados os métodos jurídico-dogmático e jurídico-teórico, dividindo o trabalho em três partes. Foram consultados materiais nacionais e estrangeiros, jurídicos e tecnológicos, especialmente da União Europeia, do Reino Unido e dos EUA, além de projetos, orientações, guias e planos de entidades públicas estrangeiras.

Como resposta ao problema da pesquisa, as *principais peculiaridades* encontradas foram: as ausências legal, jurisprudencial e de orientações sobre a proteção de dados pessoais em cidades inteligentes, gerando a necessidade de adequação do sistema de proteção de dados pessoais brasileiro; a divergência internacional sobre os direitos de proteção de dados pessoais e de privacidade, dificultando a implantação tecnológica estrangeira na cidade; a limitação tecnológica em garantir a segurança, os direitos e as liberdades civis juridicamente protegidos e; o risco de monitoramento excessivo sobre a vida dos cidadãos, protagonizado pelo governo ou por empresas privadas.

Já as *principais medidas protetivas* encontradas foram: a imposição do *Privacy By Design* desde a concepção do produto ou serviço de TIC; a criação de regras específicas para uso de dados pessoais sensíveis no ambiente digital; a promoção de programas criativos de conscientização sobre a proteção dos dados pessoais; o organograma de DPO's para fiscalizar e orientar o Poder Público; a confecção de um plano municipal de implantação de tecnologia *smart city*, contento avaliações de impacto de proteção de dados pessoais e o envolvimento de todos os componentes da sociedade; a adoção de um modelo contratual para empresas estrangeiras que garanta a observância do sistema de proteção dos dados pessoais brasileiro no ambiente urbano.

Palavras-chave. *smart city*; proteção de dados pessoais; cidade

ABSTRACT

The deployment of smart city technology in foreign cities is promoting the collection and processing of personal data on a large scale. This caused a global concern about the risks of violating rights and guarantees of personal data protection systems in the urban environment.

Some Brazilian cities are in the initial phase of using the smart city, which shows the urgency of legal studies about the data protection in this environment. Therefore, the problem of this work is to investigate the peculiarities of data protection in the implementation of a smart city technology in the city, identifying challenges and present measures to deal with these issues in Brazil.

For that, the legal-dogmatic and legal-theoretical methods were used, The work was divided into three parts. National and foreign legal and technological materials were consulted, especially from the European Union, the United Kingdom and the USA, as well as projects, guidelines, guides and plans from foreign public entities.

In response to the research problem, the main peculiarities found were: the absence of legal, jurisprudential and guidance on the data protection in smart cities, and needs to adapt the Brazilian personal data protection system; the international conflicts on personal data protection and privacy rights, making it difficult to implement foreign technology in the city; the technological limitation to ensure security, rights and civil liberties; bulk surveillance of citizens' lives by the government or private companies.

The main protective measures found were: the imposition of Privacy By Design from the conception of the ICT product or service; the creation of specific rules for the use of sensitive personal data in the digital environment; the promotion of creative programs about the protection of personal data; the DPO’s organization structure to supervise and guide the Public Authorities; the municipal plan for the implementation of smart city technology in the urban environment, containing data protection impact assessment and the participation of all components of society; the creation of a contractual model for foreign companies that guarantees compliance with the Brazilian personal data protection system in the urban environment.

Key words. smart city; protection of personal data; city

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACLU – *American Civil Liberties*

ADI – Ação Direta de Inconstitucionalidade

ADPF – Ação de Descumprimento de Preceito Fundamental

AEPD – Autoridade Europeia para a Proteção de Dados

AIPD – Avaliação de impacto de proteção de dados

ANPD – Autoridade Nacional de Proteção de Dados

ANATEL – Agência Nacional de Telecomunicações

AoT – *Array of Things*

AVC – Acidente Vascular Cerebral

BCB – Banco Central do Brasil

CC – Código Civil (Lei nº 10.406/2002)

CCTV – *Closed-circuit Television*

CDC – Código de Defesa do Consumidor (Lei nº 8.078/1990)

CF/88 – Constituição Federal

CNPD – Comissão Nacional de Proteção de Dados

COMPAS – *Correctional Offender Management Profiling for Alternative Sanction*s

DTG – *Dirección General de Tráfico*

DPC – *Data Protection Commissioner*

DPO – *Data protection officer*

DPIA – *Data protection impact assessments*

Ed. – Edição

EECC – *European Electronic Communications Code*

EFTA – *European Free Trade Association*

EHR – *Electronic Health Record*

ENISA – *European Union Agency for Cybersecurity*

EUA – Estados Unidos da América

GDPR – *General Data Protection Regulation*

IA – Inteligência Artificial

IBGE – Instituto Brasileiro de Geografia e Pesquisa

ICO – *Information Commissioner's Ofice*

IDEC – Instituto Brasileiro de Defesa ao Consumidor

Idem – Mesmo autor

I~HD – *European Institute for Innovation through Health Data*

IoT – *Internet of Things*

ITU – *International Telecommunication Union*

LAI – Lei de Acesso à Informação (Lei nº 12.527/2011)

LED – *Light Emitting Diode*

LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

LPG – *London Plan Guidance*

LRP – Lei dos Registros Públicos (Lei nº 6.015/1973)

MCI – Marco Civil da Internet (Lei nº 12.965/2014)

MECTIC – Ministério de Estado da Ciência, Tecnologia, Inovações e Comunicações

MP – Ministério Público

N. – Número

NSA – *National Security Agency*

NYCLU – *New York Civil Liberties Union*

OAIC – *Office of the Australian Information Commissioner*

Org. – Organizadores

P. – Página

PDF – *Portable Document Format*

PDPA – *Personal Data Protection Act*

PDPC – *Personal Data Protecition Commission*

PL – Projeto de Lei

PLC – *Public London Charter*

PNCI – Política Nacional de Cidades Inteligentes

PNIC – Plano Nacional de Internet das Coisas

RIPA – *Regulation of Investigatory Powers Act 2000*

SC – *Smart City*

SCC – *Standard Contractual Clauses*

SI – Segurança da Informação

SSC – *Smart Sustentable City*

STJ – Superior Tribunal de Justiça

STF – Supremo Tribunal Federal

SURE – *Smart Urban Security and Event Resilience*

TIC –Tecnologia da Informação e Comunicação

TJSP –Tribunal de Justiça de São Paulo

UE – União Europeia

UK – *United Kingdom*

UK GDPR – United Kingdom *General Data Protection Regulation*

USP – Universidade de São Paulo

V. – Volume

3Vs – Volume, a variedade e a velocidade

SUMÁRIO

INTRODUÇÃO:

Há muito tempo, mesmo que de forma simples e em menor escala, as cidades coletam e utilizam dados para diversas finalidades. Um exemplo é o censo nacional brasileiro que, desde 1872, coleta e analisa dados sobre a vida da população para fins de políticas públicas e tomadas de decisões de investimentos da iniciativa privada[1].

Nas últimas décadas do século XX, a revolução da Tecnologia da Informação (ou simplesmente TIC) transformou a economia global, que agora é baseada na capacidade de gerar, processar e aplicar, de forma eficiente, as informações. Assim, as principais atividades produtivas, seja de prestação de serviço ou de fornecimento de produtos, têm a informação como um material indispensável[2].

Impulsionada pela indústria 4.0[3], essa mudança também abarcou os serviços públicos e produtos destinados ao ambiente urbano, e vem alterando, rapidamente, a forma de vida em sociedade. Em meio à geração e coleta de dados em larga escala, surgem desafios para garantir as liberdades civis e os direitos fundamentais, especialmente a proteção dos dados pessoais.

Desse modo*, este trabalho estuda quais são as principais peculiaridades da proteção de dados pessoais em cidades "inteligentes", que tipo de desafio elas acarretam e como o Direito deve tratar essas questões*. Aborda, especificamente, situações de uso de dados pessoais por tecnologia *smart city* (ou cidade inteligente) implantada em cidades.

Frisa-se, não é analisada a proteção de dados pessoais em tecnologia inserida nos ambientes rural e privado, mas, tão somente, em tecnologias implantadas nas cidades. De igual

---

[1] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Comitê de estatísticas sociais**. 2023. Disponível em: https://ces.ibge.gov.br/apresentacao/portarias/200-comite-de-estatisticas-sociais/base-de-dados/1146-censo-demografico.html#:~:text=O%20Censo%20Demogr%C3%A1fico%20tem%20por,ou%20de%20qualquer%20n%C3%ADvel%20de

[2] CASTELLS, Manuel. **A era da informação: Economia, sociedade e cultura. A sociedade em rede.** Vol. 1. Ed. Paz e Terra LTDA. São Paulo. 1999. 87 p.

[3] "(...) acredito que hoje estamos no início de uma quarta revolução industrial. Ela teve início na virada do século e baseia-se na revolução digital. É caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina). As tecnologias digitais, fundamentadas no computador, software e redes, não são novas, mas estão causando rupturas à terceira revolução industrial; estão se tornando mais sofisticadas e integradas e, consequentemente, transformando a sociedade e a economia global. (...) A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos. Nessa revolução, as tecnologias emergentes e as inovações generalizadas são difundidas muito mais rápida e amplamente do que nas anteriores, as quais continuam a desdobrar-se em algumas partes do mundo." SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016. 16-17 p.

forma, não constituem objeto deste estudo os casos em que a tecnologia *smart city* utiliza dados anônimos, pois o foco está nas situações que envolvem os dados pessoais.

Destaca-se, também, que este trabalho não tem a pretensão de aprofundar nos conceitos das tecnologias, mas relacioná-los com a proteção de dados pessoais em cidades inteligentes. O foco é o direito a Proteção de Dados Pessoais, os princípios e objetivo do Direito Urbanístico, e a relação dessas disciplinas jurídicas com a *smart city*.

Como *hipótese*, os desafios específicos à proteção de dados gerados pelo ambiente tecnológico urbano são: as ausências de dispositivos legislativos específicos, orientações e entendimentos jurisprudenciais sobre a proteção de dados pessoais em cidades "inteligentes"; a distinção de entendimentos entre os países sobre a proteção de dados pessoais e a privacidade, gerando um risco na utilização de tecnologia *smart city* estrangeira nas cidades brasileiras; as limitações atuais dessa tecnologia na garantia dos princípios e direitos impostos pelo sistema de proteção dos dados pessoais; as práticas ilegais de compartilhamento dos dados e o desvio de finalidade; a deficiência na fiscalização das operações que envolvem dados pessoais no ambiente urbano; O monitoramento excessivo nas cidades, ocasionado pela tecnologia inserida no ambiente urbano e; o risco de discriminação na tecnologia de cidades inteligentes.

Para alcançar os seus objetivos, este trabalho utiliza duas metodologias, quais sejam, a jurídico-dogmática e a jurídico-teórica. A primeira terá como objeto a análise e interpretação dos dispositivos inerentes à temática e a segunda estudará a revisão bibliográfica para análise de conceitos e teorias do ordenamento, bem como das tecnologias de cidade inteligente e de suas ferramentas.

Quanto ao marco teórico para o Direito de Proteção de Dados Pessoais, adotam-se como pilares a Constituição Brasileira de 1988, a Lei Geral de Proteção de Dados brasileira (LGPD), o Marco Civil da Internet (MCI), a Lei de Acesso à Informação (LAI), o Plano Nacional de Internet das Coisas (PNIC), O Plano Nacional de Cidade Inteligente (PNCI), o Decreto que dispõe sobre a Governança da Segurança da Informação e demais leis, entendimentos jurisprudenciais e da Autoridade Nacional de Proteção de Dados (ANPD), além das doutrinas que formam o sistema jurídico de proteção de dados brasileiro.

Como fonte jurídica internacional adotam-se a legislação, doutrina, jurisprudência e entendimentos de autoridades estadunidenses e europeias, e, pontualmente, leis e entendimentos de autoridades e de órgãos internacionais do Reino Unido, da Australia e de Singapura.

Já para o Direito Urbanístico, além da Constituição Brasileira de 1988, estuda a Lei nº 10.257/2001, conhecida como Estatuto da Cidade e doutrinas sobre o tema. De forma pontual, utiliza-se a Lei de nº 13.089/2015, denominada Estatuto da Metrópole.

Usa-se as literaturas nacional e internacional sobre as cidades inteligentes e as tecnologias que lhe são correlatas, tais como, a *Internet das Coisas* (*Internet of Things* - IoT)[4] e o *big data*[5]. Também se utiliza materiais, dos governos nacional e estrangeiros, sobre a implantação da tecnologia *smart city* no ambiente urbano, como, projetos, guias e reportagens.

Este trabalho é estruturado em três partes além da Introdução. O Capítulo I se inicia com a construção de um conceito para a cidade inteligente; seguida pelas peculiaridades de um ambiente urbano tecnológico que o diferencia de uma cidade tradicional e; finaliza apontando desafios à proteção de dados pessoais no ambiente tecnológico urbano. Já o Capítulo II aprofunda sobre cada um dos desafios encontrados, indicando pontos de conflito entre a tecnologia *smart city* e o Direito, especialmente sobre os sistemas de proteção de dados pessoais. O Capítulo III apresenta medidas estrangeiras criativas de mitigação e prevenção às violações contra os direitos de proteção dos dados pessoais. Finalmente, tem-se a Conclusão.

[4] "Os dispositivos de Internet das Coisas nada mais são do que pequenos microcomputadores em sua essência que se encontram conectados à Internet e Cloud, buscando facilitar ou complicar ainda mais as nossas vidas. O termo IoT vem da terminologia, em língua inglesa "Internet of Things", ou Internet das Coisas, esse termo soa um pouco estranho quando traduzimos para o português, ainda mais porque não considero um microcomputador, na essência da palavra, como uma "coisa", mas sim uma máquina complexa e inteligente que implementa aplicações que podem ser extremamente avançadas. É assim quando um dispositivo médico, como um marcapasso, auxilia na manutenção do bem mais precioso que existe, que é a vida humana. Além disso, esse pequeno dispositivo com capacidade computacional se integra à internet permitindo avisar a um centro médico quando algo de errado está acontecendo com o paciente. A IoT colabora para trazer conforto ao nosso cotidiano estressante, em especial nas grandes metrópoles, a comodidade de, através do seu dispositivo móvel, poder acionar outros em sua casa para controlar a climatização (ar-condicionado), monitorar remotamente sua residência através de câmeras inteligentes e dispositivos avançados, como sensores de presença, controle de iluminação e tantas milhares de aplicações que estão presentes no conceito de casas inteligentes." MORAIS, Alexandre de; HAYASHI, Vitor Takashi. **Segurança em Iot. Entendendo os riscos e ameaças em Internet das Coisas**. Editora Alta Books. 2021 13 p.

[5]"Big Data is, in many ways, a poor term. As Lev Manovich (2011) observes, it has been used in the science store fer to data sets large enough to require super computers, although now vast sets of data can be analyzed on desktop computers with standard software. There is little doubt that the quantities of data now available are indeed large, but that's not the most relevant Characteristic of this new data ecosystem. Big Data is not able not because of its size, but because of its relationality to other data. Due to efforts to mine and aggregate data, Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about na individual, about individuals in relation to others, about groups of people, or Simply about the structure of information it self". BOYD, Danah, KATE, Crawford, **Six Provocations for Big Data**. 21/09/2011 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431. Já para o Gartner IT glossary Big data., "Big data is high-volume, high-velocity and high-variety information as sets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making". GARTNER. **Gartner Glossary. Information Technology**. **Big Data**. Disponível em: http://www.gartner.com/it-glossary/big-data

CAPÍTULO I: A CIDADE INTELIGENTE

1.1. Os conceitos de cidade inteligente

Atualmente, *não há consenso* na literatura técnica sobre o significado de cidade inteligente. Várias organizações, públicas e privadas, possuem a sua própria atribuição, sendo que, só no ano de 2014, foram catalogadas mais de 100 conceituações distintas[6].

Não está entre os objetivos deste trabalho analisar todos estes conceitos e, tampouco, encontrar uma definição padrão para todas as cidades inteligentes, até porque, pelos motivos expostos a seguir, essa pretensão parece inexequível, ao menos atualmente. Deste modo, a proposta de estudo é encontrar um *conceito amplo*, capaz de abranger o *máximo de elementos possíveis*, e que *atenda às necessidades deste trabalho*.

Importa ainda destacar que as tecnologias de cidades inteligentes também podem ser aproveitadas no campo[7]. Porém, enfatiza-se, não é objeto desse trabalho a inserção tecnológica na área rural, mas, tão somente, no ambiente urbano, por opção metodológica do autor.

Dito isso, este tópico verifica, inicialmente, alguns conceitos de *cidade*, até mesmo para diferenciá-los da cidade *inteligente*. Após, investiga diretrizes do Direito Urbanístico importantes para os propósitos da cidade, traçando um paralelo com a cidade inteligente. Por fim, analisa alguns significados de cidades inteligentes, até formar um conceito próprio, que atenda às finalidades deste trabalho.

Identificar características comuns existentes em todas as cidades é um desafio complexo, tendo em vista as várias diferenças ocasionadas por épocas, culturas, climas e geografias distintos. O dicionário Houaiss[8] define cidade como:

> *Aglomeração humana de certa importância, localizada numa área geográfica circunscrita e que tem numerosas casas, próximas entre si, destinadas à moradia e/ou a atividades culturais, mercantis, industriais, financeiras e a outras não relacionadas com a exploração direta do solo"*

---

[6]INTERNATIONAL TELECOMMUNICATION UNION. **Smart sustainable cites: Na analysis of definitions.** Focus Group Technical Report. 2014.

[7]FORBES. **What Smart Cities are Learning From Smart Farms**. 27/11/2019. Disponível em: <https://www.forbes.com/sites/bayer/2019/11/27/what-smart-cities-are-learning-from-smart-farms/?sh=7d71342fac64>

[8]INSTITUTO ANTONIO HOUAISS. **Dicionário Houaiss da Língua portuguesa**. Editora Objetiva. 2008. 714 p.

Este conceito traz alguns elementos comuns das cidades, como, o *elemento espacial,* que é a área geográfica e circunscrita, intimamente ligado ao elemento da *aglomeração humana permanente*, que ocorre quando o homem domina as técnicas de plantio[9] e, daí, tem uma vida permanente em um local específico.

Afere-se também deste conceito o *elemento comercial*, representado pelas atividades econômicas industriais, comerciais e de prestação de serviços. Compara-se a cidade a um imã, pois as pessoas são atraídas para ela. Antigamente, essa atração se dava pelos templos, antes mesmo da era cristã[10]. Porém, é a partir do momento em que a cidade se organizou em função do *elemento mercado*, formando uma estrutura urbana e redefinindo os seus espaços interno e circundante, que ela atraiu grandes populações[11].

Antes da época moderna, a cidade era uma unidade autônoma, estruturada em torno de uma igreja e de suas instituições, contendo espaços de comércio, praças e moradias. Todavia, hoje a cidade é um sistema aberto, profundamente dependente de fatores externos, como questões econômicas e ambientais[12].

Aqui, ressalta o papel da tecnologia quanto ao aumento da dependência externa das cidades, especialmente com o advento da internet, das inovações tecnológicas dela decorrentes e do desenvolvimento do transporte. Inclusive, as tecnologias disruptivas[13] aumentam essa dependência, como será constatado nos próximos tópicos deste trabalho.

Por fim, o conceito do dicionário Houaiss traz o *elemento cultural*, característica comum nas cidades. A forma como são construídas as praças, templos, ruas e casas denota a história de uma comunidade, escrevendo a tradição daquele povo[14].

Devido à complexidade de identificar um conceito comum para todas as cidades do globo, há quem se limita em buscar uma definição apenas para a cidade *brasileira*. Desse modo, enumeram-se quatro elementos para o ambiente urbano brasileiro que são: a aglomeração, a permanência, o mercado e a administração pública[15].

---

[9] ROLNIK, Raquel. **O que é cidade**. 3ª edição. Editora brasiliense 1994 7 p.
[10] ROLNIK, Raquel. **O que é cidade**. 3ª edição. Editora brasiliense 1994 13 p.
[11] ROLNIK, Raquel. **O que é cidade**. 3ª edição. Editora brasiliense 1994. 31 p.
[12] SEGUÍN, Élida. **Estatuto da Cidade**. Editora Forense. Rio de Janeiro 2022. 35 p.
[13] Inovação Disruptiva é um processo do qual uma empresa de pequeno porte e com menos recursos desafia empresas consolidadas que possuem modelos de negócios estabelecidos, através de um serviço mais eficiente com um preço competitivo, criando um novo mercado e rompendo com o anterior. CHRISTENSEN, Clayton M.; RAYNOR, Michael E.; MCDONALD, Rory. **What is disruptive innovation***?* Harvard Business Review. 2015.
[14] ROLNIK, Raquel. **O que é cidade.** 3ª edição. Editora brasiliense 1994. 17 p.
[15] LENCIONI, Sandra. **Observações sobre o conceito de Cidade e Urbano**. GEOUSP – Espaço e Tempo. São Paulo, n º 24, 2008. 116 p.

Destaca-se o último elemento supracitado, qual seja, a administração pública. Desde a origem da cidade, há uma relação de submissão do cidadão para com o poder central, que fica responsável por prover segurança e outros serviços essenciais.

Nos dias atuais, este poder é exercido pela administração pública e é limitado por um ordenamento de princípios e regras.[16] Um dos pilares desse complexo normativo é o Direito Urbanístico, que empresta vários de seus elementos para os conceitos de cidade inteligente, como se mostra nos próximos parágrafos.

Descrito como uma ciência social interdisciplinar, o Direito Urbanístico tem por objeto *o ordenamento da vida social nas suas referências espaciais, tanto para a cidade como entre seus habitantes*[17]. É a normatização do espaço urbano, com o objetivo de propiciar ao cidadão as melhores condições de vida em comunidade.[18]

Todavia, o Direito Urbanístico se modernizou e ultrapassou os limites da cidade, passando a abranger projetos de estruturação de portes regionais que incluem o campo e outros aspectos que vão além do espaço físico do território[19]. Talvez, futuramente, com a implantação em massa das tecnologias de cidades inteligentes, este conceito seja o mais adequado.

De qualquer modo, o *elemento comum* extraído dos conceitos de Direito Urbanístico, e que é fundamental na definição de cidade inteligente, é o cidadão como ponto central do ambiente urbano. O objetivo principal de uma cidade é o de propiciar as melhores condições possíveis para a vida do ser humano em sociedade.

Toda e qualquer política urbana, inclusive aquela que visa à inserção tecnológica no ambiente urbano, deve ter como finalidade principal o bem-estar do cidadão. Esta concepção tem origem no caput do artigo 182 da Carta Magna brasileira, dispositivo basilar do Direito Urbanístico:

> *Art. 182. A política de desenvolvimento urbano, executada pelo Poder Público municipal, conforme diretrizes gerais fixadas em lei, tem por objetivo ordenar o pleno desenvolvimento das funções sociais da cidade e garantir o* ***bem- estar de seus habitantes (negrito nosso).***

---

[16] ROLNIK, Raquel. **O que é cidade**. Editora brasiliense. 3ª edição. 1994 23-24 p.
[17] SEGUÍN, Élida. **Estatuto da Cidade**. Rio de Janeiro. Editora Forense. 2022. 13 p.
[18]"O Direito Urbanístico é o conjunto de normas destinadas a dispor sobre a ordenação da Cidade, sobre a ocupação do espaço urbano de maneira justa e regular, procurando as condições melhores de edificação, habitação, trabalho, circulação e lazer. Tem por objeto organizar os espaços habitáveis, de modo a propiciar melhores condições de vida ao homem na comunidade". LIRA, Ricardo Pereira. **Direito Urbanístico, Estatuto da Cidade e regularização fundiária.** Revista de Direito da Cidade. Vol. 1. Disponível em: < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.e-publicacoes.uerj.br/index.php/rdc/article/viewFile/10493/8265> 264 p.
[19]MUKAI, Toshio. **Direito e legislação urbanística no Brasil.** Editora Saraiva. São Paulo. 1988 p.3

O artigo constitucional supracitado delegou ao legislador a criação de lei específica para fixar diretrizes gerais ao desenvolvimento urbano. Esta é a lei de nº 10.257 de 10 de junho de 2001, denominada Estatuto da Cidade, que tem como objetivo regular o *uso da propriedade urbana*[20] *em prol do bem coletivo, da segurança e do bem-estar dos cidadãos, bem como do equilíbrio ambiental*[21].

Em seu artigo 2º, estão as diretrizes gerais da política urbana. Este tópico analisa apenas o seu caput e os incisos que trazem elementos importantes para o conceito de cidade inteligente.

Os princípios da função social da cidade e da função social da propriedade urbana estão no caput do artigo 2º[22] e impõem deveres ao Estado e ao particular proprietário do imóvel urbano. A função social da cidade tem como premissa o fornecimento universal de condições de uma vida plena ao cidadão, como os acessos ao meio ambiente saudável, aos serviços essenciais e à infraestrutura urbana.[23]

Já a função social da propriedade impõe ao proprietário do imóvel urbano, seja ele o Estado ou o particular, um dever de zelo urbanístico, de redução de desigualdades nos centros urbanos. O titular do domínio se submete às regras do Estatuto da Cidade e do ordenamento municipal quando pretende edificar ou alterar as condições do seu imóvel[24].

O objetivo principal da função social da propriedade é o de garantir o emprego adequado das riquezas[25]. A concretização da função social da propriedade urbana se dá por meio de três vias, quais sejam: a proteção de direitos difusos, como, o meio ambiente e a urbanização

---

[20]A questão geográfica não é um fator determinante de diferenciação entre a propriedade urbana e a propriedade rural. O Código Tributário Nacional diferencia a propriedade urbana da propriedade rural em seu artigo 32 § 1, referente à cobrança do IPTU: "Art. 32. O imposto, de competência dos Municípios, sobre a propriedade predial e territorial urbana tem como fato gerador a propriedade, o domínio útil ou a posse de bem imóvel por natureza ou por acessão física, como definido na lei civil, localizado na zona urbana do Município.§ 1º Para os efeitos deste imposto, entende-se como zona urbana a definida em lei municipal; observado o requisito mínimo da existência de melhoramentos indicados em pelo menos 2 (dois) dos incisos seguintes, construídos ou mantidos pelo Poder Público: I - meio-fio ou calçamento, com canalização de águas pluviais: II - abastecimento de água; III - sistema de esgotos sanitários; IV - rede de iluminação pública, com ou sem posteamento para distribuição domiciliar; V - escola primária ou posto de saúde a uma distância máxima de 3 (três) quilômetros do imóvel considerado".

[21]Art. 1º "Parágrafo único. Para todos os efeitos, esta Lei, denominada Estatuto da Cidade, estabelece normas de ordem pública e interesse social que regulam o uso da propriedade urbana em prol do bem coletivo, da segurança e do bem-estar dos cidadãos, bem como do equilíbrio ambiental". **Lei de nº 10.257/2001, Estatuto da Cidade**.

[22]"Art. 2º A política urbana tem por objetivo ordenar o pleno desenvolvimento das funções sociais da cidade e da propriedade urbana, mediante as seguintes diretrizes gerais:" **Lei de nº 10.257/2001**. **Estatuto da Cidade.**

[23] RODRIGUES, Arlete Moysés. **Estatuto da Cidade: função social da cidade e da propriedade. Alguns aspectos sobre a população urbana e espaço.** Caderno Metrópole. N 12. 2 sem. 2004. 9-25 p.

[24] BIASI, Danielle Portugal de. **Propriedade: reconstruções na era do acesso e compartilhamento**. 6ª edição. Indaiatuba, SP. Editora Foco 2022. Posição 2148 e 2152

[25] BIASI, Danielle Portugal de**. Propriedade: reconstruções na era do acesso e compartilhamento**. 6ª edição. Indaiatuba, SP. Editora Foco 2022. Posição 2380

planejada; a promoção dos direitos sociais, como, a moradia e o trabalho e; o desenvolvimento econômico para a promoção de novos negócios[26].

Hoje, já se sabe do grande potencial das tecnologias em aumentar a eficiência dos serviços. Um exemplo é o Airbnb, que inovou o setor de locação por temporada através da eliminação da figura do intermediário, aproximando o locador do locatário e criando oportunidades. Esta plataforma digital deu utilidade a vários imóveis em desuso, o que desenvolveu o comércio em regiões menos favorecidas ou afastadas e fortaleceu a função social da propriedade[27].

A tecnologia é um dos pilares da economia do compartilhamento[28] do qual as pessoas procuram ter experiências e não coisas. Não é importante ter o domínio sobre o imóvel, mas, sim, o direito de acesso[29] a ele. Essa nova forma negocial se tornou atraente tanto pela sua fluidez como pela facilidade de alcance a novos bens.

A economia do compartilhamento envolve bens móveis e imóveis, corpóreos e incorpóreos. Os dados fomentam os novos modelos de negócio, assim como ocorre nas cidades inteligentes, e o seu uso ganha novo sentido com a Lei Geral de Proteção de Dados Pessoais, estudada a seguir, especificamente no ambiente urbano.

O princípio das cidades sustentáveis, constante do inciso I[30] do artigo 2º da Lei 10.257/2011, é diretamente ligado à função social da cidade e defende a conservação dos direitos do cidadão para as presentes e futuras gerações. A ideia de sustentabilidade é um dos focos de desenvolvimento da tecnologia em cidades inteligentes, que busca otimizar os serviços urbanos gastando menos recursos.

---

[26] BIASI, Danielle Portugal de. Propriedade: **reconstruções na era do acesso e compartilhamento**. 6ª edição. Indaiatuba, SP. Editora Foco 2022. Posição 2148 e 2152

[27] BIASI, Danielle Portugal de. Propriedade: **reconstruções na era do acesso e compartilhamento**. 6ª edição. Indaiatuba, SP. Editora Foco 2022. Posição 3191 e seguintes

[28] Para Carlos Affonso Pereira de Souza e Ronaldo Lemos**, "**a economia do compartilhamento está baseada no uso de tecnologia da informação em prol da otimização do uso de recursos através de sua redistribuição, compartilhamento e aproveitamento de suas capacidades excedentes". SOUZA, Carlos Affonso Pereira; LEMOS, Ronaldo. **Aspectos jurídicos da economia do compartilhamento: função social e tutela da confiança**. Vol. 08. Revista de Direito da Cidade. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.e-publicacoes.uerj.br/index.php/rdc/article/viewFile/25740/19159 1757-1777 p.

[29] BIASI, Danielle Portugal de. Propriedade: **reconstruções na era do acesso e compartilhamento**. 6ª edição. Indaiatuba, SP. Editora Foco 2022. Posição 4013

[30] Art. 2º "inciso I – garantia do direito a cidades sustentáveis, entendido como o direito à terra urbana, à moradia, ao saneamento ambiental, à infraestrutura urbana, ao transporte e aos serviços públicos, ao trabalho e ao lazer, para as presentes e futuras gerações;" Lei 10.257/2001

O inciso II[31] desse mesmo artigo se refere ao princípio da participação popular sobre projetos de desenvolvimento urbano. O envolvimento da população deve ocorrer em todas as etapas do projeto, ou seja, da criação à execução.

Em se tratando de projetos de implantação de tecnologia *smart city* em ambiente urbano, a participação popular é obrigatória. Apesar de trazer muitos benefícios, a tecnologia *smart city* representa riscos a alguns direitos dos cidadãos que podem optar pela não implantação, gerando grandes prejuízos econômicos às empresas e ao Estado que investem sem a prévia consulta popular. [32]

O inciso III[33] dispõe sobre o desenvolvimento de um ambiente cooperativo entre os componentes de uma cidade. O princípio da cooperação busca unir o governo, a iniciativa privada, o meio acadêmico e todos os demais setores da sociedade na busca pelo aprimoramento de serviços e produtos em ambiente urbano.

Este princípio está intimamente ligado à implantação de tecnologia *smart city* em cidades como, por exemplo, através da utilização de plataforma de compartilhamento de dados entre os diversos setores da sociedade, estudada em momento posterior. A troca de informações possibilita o desenvolvimento conjunto de serviços e produtos urbanos.

O inciso IV[34] dispõe sobre o princípio do planejamento para o desenvolvimento da cidade, que tem por objetivo a distribuição espacial equilibrada, tanto da população quanto das atividades econômicas do município. O planejamento eficiente da cidade evita o crescimento urbano desordenado, uma das causas da desigualdade social e econômica do ambiente urbano.

A implantação tecnológica *smart city* pode ser benéfica para o planejamento urbano como, por exemplo, a produção de informações em massa e em tempo real, conforme se estuda a seguir. Isto aprimora o gerenciamento do município em vários de seus serviços e fornece mais subsídios para o seu planejamento de crescimento urbano.

Apesar da impossibilidade de criar um conceito único de cidade que contemple todas as cidades do mundo, é possível identificar elementos comuns, quais sejam, a aglomeração humana permanente, o aspecto cultural e único de cada região, o desenvolvimento econômico,

---

[31] art. 2º "inciso II - gestão democrática por meio da participação da população e de associações representativas dos vários segmentos da comunidade na formulação, execução e acompanhamento de planos, programas e projetos de desenvolvimento urbano;" **Lei 10.257/2001. Estatuto da Cidade.**

[32] LIMA, Gabriel Ribeiro de. **Proteção de Dados em Cidade inteligente: o caso Sidewalk Labs (Google) em Toronto**. Editora Dialética LTDA. 2023 p 243 e seguintes.

[33] "Art. 2º inciso III - cooperação entre os governos, a iniciativa privada e os demais setores da sociedade no processo de urbanização, em atendimento ao interesse social;" **Lei 10.257/2001. Estatuto da Cidade.**

[34] "Art. 2º inciso IV - planejamento do desenvolvimento das cidades, da distribuição espacial da população e das atividades econômicas do Município e do território sob sua área de influência, de modo a evitar e corrigir as distorções do crescimento urbano e seus efeitos negativos sobre o meio ambiente;" **Lei 10.257/2001. Estatuto da Cidade.**

o poder central, no Brasil representado pela Administração Pública, e a infraestrutura urbana. Estes elementos devem estar presentes na concepção de cidade inteligente.

Desse modo, um bom conceito de cidade deve abranger todos os elementos comuns possíveis, além daqueles trazidos pelo Direito Urbanístico. Assim, o termo cidade consiste em uma área *geográfica circunscrita*, preenchida por uma *infraestrutura urbana sustentável* e *habitada por uma aglomeração humana permanente*, que possui *atividades* de desenvolvimento urbano, cultural, econômico, social, e ambiental, protegidas, *planejadas e organizadas* pela administração pública em cooperação com os demais setores da sociedade, cujo *objetivo principal é o bem-estar do cidadão*.

A cidade inteligente deve ter o mesmo objetivo da cidade tradicional, que é o bem-estar do cidadão. Este objetivo e as diretrizes principiológicas do Direito Urbanístico que são as funções sociais da cidade e da propriedade, a sustentabilidade, a participação popular, a cooperação e o planejamento, devem ser lembrados no significado de cidade inteligente.

Na maioria dos casos estudados, a definição de cidade inteligente foi fortemente influenciada pelo interesse da própria organização que criou o conceito. Por existirem interesses conflitantes por trás do debate terminológico sobre este termo, vários conceitos são incompletos.

Um exemplo de equívoco conceitual de *smart city* é o do *Ranking Connected Smart Cities*, realizado no Brasil pelas empresas *Necta e Urban Sytems.* De acordo com o site do evento, *smart city* é o desenvolvimento da conectividade entre os diversos setores de uma sociedade, como saúde, mobilidade urbana e segurança[35].

Este conceito sequer possui os atributos comuns de uma cidade tradicional, necessários para a construção da concepção de cidade inteligente. Afinal, cidade inteligente também é uma cidade.

Ademais, como se verá a seguir, a tecnologia *smart ctiy* vai muito além de uma mera conexão entre serviços urbanos. Sua inserção no ambiente urbano envolve, além de vários componentes tecnológicos, o desenvolvimento de outros elementos que compõem a sociedade.

Inicialmente, o rótulo "cidade inteligente" foi um jargão utilizado por consultores, profissionais de marketing e provedores de serviços tecnológicos para comercializar os seus produtos e serviços inseridos no ambiente urbano.[36] Na literatura técnica, cidade inteligente

---

[35] RANKING CONNECTED SMART CITIES. **Sobre o Ranking Connected Smart Cities**, Disponível em: https://ranking.connectedsmartcities.com.br/

[36] PRARAHAJ, Sarbeswar; HAN, Hoon. *City, Culture e Society*. **Cutting through the clutter of smart city definitions: A reading into the smart city perceptions in India**. Volume 18. September 2019. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1877916618302935

pode significar uma tecnologia voltada ou para as necessidades do cidadão ou para a iniciativa privada ou para o desenvolvimento de cidades[37].

A definição de cidade inteligente centralizada no cidadão é comumente encontrada na doutrina europeia. Entende-se que apenas a tecnologia não é capaz de enfrentar os desafios de uma cidade, sendo igualmente necessário haver mudanças substanciais, tanto no estilo de vida dos cidadãos como nas políticas públicas, para alcançar um resultado satisfatório, qual seja, a criação de um ambiente tecnológico urbano capaz de atender às necessidades da comunidade e, ao mesmo tempo, de ser autossustentável e não trazer prejuízos ao meio ambiente.

Já na iniciativa privada, o conceito de cidade inteligente está ligado à suposição de que somente a tecnologia oferece a solução para todos os antigos problemas enfrentados pelas cidades. Além disso, geralmente, o termo está vinculado à utilização de uma infraestrutura tecnológica complexa que se vale da internet das coisas, do *big data* e da inteligência artificial para promover o desenvolvimento urbano.

Entende-se que os dois primeiros conceitos não são conflitantes, mas há neles a omissão de alguns elementos. Pelo interesse natural de comercialização, há uma super valorização da tecnologia, que não é capaz de suprir todas as necessidades de uma cidade sem o esforço conjunto de todos os seus elementos.

Os princípios da cooperação e da participação popular trazidos pelo direito urbanístico são fundamentais para o sucesso da implantação de uma cidade inteligente. Portanto, o conceito da iniciativa privada é incompleto em comparação ao europeu.

Além dessas duas concepções, o termo cidade inteligente também pode se referir ao potencial da tecnologia em melhorar a eficiência de um ambiente urbano em comparação às cidades tradicionais. Dessa forma, "*smart"* é entendido como *ganho de eficiência*, onde o valor das novas tecnologias é definido pela sua capacidade para identificar e superar (ou reduzir) as deficiências existentes nas cidades tradicionais[38].

No entanto, o significado de cidade inteligente deve englobar *todos* os elementos inseridos no ambiente urbano, tendo como principais o cidadão, as empresas privadas, a inovação tecnológica, a sustentabilidade, os desenvolvimentos humano, econômico e social, os serviços públicos, os órgãos governamentais, o meio ambiente, a privacidade e a proteção de

[37]COHEN, Boyd. **The 3 Genarations of Smart Cities**. Fast Company. 08/10/2015. Disponível em: https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities
[38]ZIOSI, Marta; HEWIT, Benjamin; JUNEJA, Prathm e outros. **Smart Cities: Reviewing the Debate about their Ethical Implications**. 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001761

dados pessoais. É claro que as duas últimas concepções apresentadas não possuem a maioria desses elementos e, por isso, estão defasadas.

Com efeito, apesar de a visão de cidade inteligente voltada para o cidadão ser mais abrangente que as demais concepções, ela também não é completa. Falta-lhe, especialmente, aspectos que apoiem o desenvolvimento econômico, social, a inovação tecnológica e a livre iniciativa.

Além dos interesses conflitantes, outra questão que dificulta a criação de um padrão conceitual de cidade inteligente são as diferentes perspectivas sociais sobre a tecnologia inserida nas cidades ao redor do mundo[39]. Cada ambiente urbano tem as suas peculiaridades, que são criadas pela cultura, pelos costumes e por fatores geográficos de cada região. Portanto, cada cidade tem as suas necessidades, os seus recursos disponíveis e as suas preferências para a inovação tecnológica.

Por serem regiões de grande influência no Brasil, interessa verificar para esta pesquisa como as legislações dos EUA e da União Europeia regulam a cidade inteligente. Em 2021, o *U. S. Congress*, por meio do *Smart Cities and Communities Act of 2021*, conceituou *smart city:*

> *This bill establishes programs for the implementation and use of smart technologies and systems in communities of various sizes. A smart city or community is one in which innovative, advanced, and trustworthy information, communication, and energy technologies are applied to (1) improve the health and quality of life of residents; (2) increase efficiency of operations and services; (3) promote economic growth; and (4) create a community that is safer and more secure, equitable, sustainable, resilient, livable, and workable.* [40]

O significado atribuído à cidade inteligente pelo *U. S. Congress* tem como principal elemento a tecnologia, supostamente responsável pelo ganho de eficiência dos serviços na cidade. Talvez, esta abordagem seja pelo forte poder de influência das empresas de TIC[41] americanas.

---

[39]PRARAHAJ, Sarbeswar; HAN, Hoon. **City, Culture e Society. Cutting through the clutter of smart city definitions: A reading into the smart city perceptions in India**. Vol. 18. September 2019. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1877916618302935

[40]CONGRESS.GOV. **H.R.3386 - Smart Cities and Communities** Act of 2021. 117th Congress (2021-2021) disponível em: <https://www.congress.gov/bill/117th-congress/house-bill/3386?s=1&r=11>

[41] "TIC" é a abreviação de Tecnologia da Informação e Comunicação. Este termo pode ser definido como um conjunto de recursos tecnológicos, utilizados de forma integrada, com um objetivo comum. São tecnologias usadas para reunir, distribuir e compartilhar informações. O desenvolvimento de hardwares e softwares para a automação e a comunicação foi potencializado pela internet. O Ministério da Gestão e Inovação de Serviços conceitua TIC como "conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos de TIC, de acordo com as premissas definidas no Anexo II desta Instrução Normativa" Dentre as categorias, estão

Já o conceito de cidade inteligente na União Europeia se aproxima de uma economia sustentável. Inclusive, a *International Telecommunication Union* (ITU)[42], agência das Nações Unidas especializada em Telecomunicações, Tecnologias da informação e Comunicação (TICs), publicou um relatório com a sua definição sobre *Smart Sustentable City* (SSC):

> *A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects.*

Tanto a perspectiva estadunidense como o entendimento europeu, representado pela ITU, trazem partes distintas e *complementares* do conceito de cidade inteligente, uma vez que o *U. S. Congress* evidencia o desenvolvimento econômico e a eficiência tecnológica e, a ITU, o desenvolvimento urbano centralizado no cidadão, no meio ambiente e nas gerações futuras.

Para o *United Kingdom Parliament*, cidade inteligente é um termo que descreve lugares que incorporam uma variedade de tecnologias, especialmente aquelas que coletam dados, para auxiliar na solução de desafios econômicos, sociais e ambientais. Geralmente, esses lugares são ambientes urbanos, mas o termo também contempla ambientes rurais[43].

Como foi dito no início deste tópico, a tecnologia de cidade inteligente pode ser utilizada no campo, mas o ambiente rural não é objeto deste estudo. Aqui, vale uma menção ao conceito do *U. S. Congress*, que diferente do parlamento do Reino Unido, não expõe, de forma expressa, a utilização da tecnologia *smart city* no campo, mas, utiliza o termo *smart community* para considerar que esta tecnologia pode ser utilizada em um ambiente que não seja a cidade.

A cidade inteligente compreende sujeitos variados, como, o governo, as universidades, as operadoras de transporte, os fornecedores de serviços públicos e privados, além de outras

---

Internet Of Things, análise de Dados, aprendizado de máquina e inteligência artificial. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS. **Conceito de Solução de TIC.** Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/conceito-de-solucao-de-tic.

[42] *"*The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.*"* INTERNATIONAL TELECOMMUNICATION UNION. **Smart sustainable cites: Na analysis of definitions**. Focus Group Technical Report. 2014. 3 p.

[43]UK PARLIAMENT. **Research Briefing, Smart Cities**. 22/09/2021. Disponível em: https://post.parliament.uk/research-briefings/post-pn-0656/

organizações[44]. As tecnologias utilizadas variam desde sensores e outros dispositivos de internet das coisas (IoT) até tecnologia 5G e outras tecnologias de conexão de dispositivos em rede.

Além disso, a tecnologia de cidade inteligente abrange tanto projetos de pequena escala de tecnologia para otimizar um serviço específico, a exemplo dos sensores de áudio que ajudam a identificar vazamento de água, até projetos de grande escala, como redes de coleta de dados em toda a cidade, para viabilizar alguma política pública.

O *Parliament* do Reino Unido adicionou elementos importantes para o conceito de cidade inteligente que são os *agentes responsáveis* por inserir a tecnologia de cidade inteligente e as diferentes escalas em que ela pode ser aplicada. Todavia, o conceito ainda carece de outros elementos, pois considera apenas a parte tecnológica da cidade inteligente, sem levar em conta fatores determinantes, como, o material humano, principal componente para a inovação tecnológica.

Kitchin[45] divide o significado de cidade inteligente em dois entendimentos distintos, embora conectados entre si. O primeiro deles se refere ao equipamento tecnológico inserido no ambiente urbano para potencializar os serviços, como, telecomunicações sem fio, serviços de utilidade controlados digitalmente e redes de sensores e câmeras que são usados para monitorar, gerenciar e regular fluxos e processos da cidade. Esse primeiro entendimento também abarca todo o processo que conecta, integra e analisa dados. Inclusive, a tecnologia que fornece toda a infraestrutura de suporte para a atividade empresarial e novas formas de empreendimento.

Já o segundo entendimento define cidade inteligente como aquela cuja economia e governança são impulsionadas pela inovação, criatividade e empreendedorismo. Aqui, TIC é uma plataforma para mobilizar e concretizar ideias e inovações, ou seja, apenas um dos atributos que classifica uma cidade como inteligente.

Desse modo, *cidade inteligente não é apenas um ambiente urbano que possui a tecnologia TIC inserida nos seus serviços públicos*. Consiste em um conjunto de fatores, dentre eles as implantações TIC, somada com os capitais humano e social e a política econômica, todos trabalhando para o desenvolvimento urbano.

Para Kitchin, o que conecta os dois entendimentos acima relatados é a prioridade dada às soluções tecnológicas para a governança e o desenvolvimento da cidade. Não é à toa que os

---

[44]UK PARLIAMENT. **Resarch Briefing, Smart Cities**. 22/09/2021. Disponível em: https://post.parliament.uk/research-briefings/post-pn-0656/

[45]KITCHIN, Rob, **The Real-Time City? Big Data and Smart Urbanism** July 3, 2013. GeoJournal 79(1):1-14, 2014, Available at SSRN: https://ssrn.com/abstract=2289141 or http://dx.doi.org/10.2139/ssrn.2289141 2 - 3 p.

principais defensores das cidades inteligentes são as grandes empresas, que pressionam os governos para a desregulação, a privatização e a abertura econômica desse mercado.

Os adeptos das correntes conceituais citadas por Kitchin identificam uma cidade inteligente através de cinco peculiaridades, sendo elas:[46] 1) a implantação generalizada de TIC no ambiente urbano; 2) o desenvolvimento urbano liderado por empresas e uma abordagem neoliberal de governança; 3) um foco nas dimensões sociais e humanas da cidade a partir de uma perspectiva de cidade criativa; 4) a adoção de uma agenda de comunidades mais inteligentes com programas voltados para aprendizagem social, educação e capital social e; 5) foco na sustentabilidade social e ambiental.

As visões relatadas por Kitchin sobre cidade inteligente têm outra característica marcante que é a importância da coleta de dados, insumo essencial para a criação e o desenvolvimento de uma cidade inteligente. Para o autor, todas as informações da cidade inteligente seriam abertas e, portanto, acessíveis a todos. Além disso, Kitchin acredita que esses dados são um material neutro e livre de ideologia política, mostrando a realidade sobre o que ocorre na cidade.

Os conceitos de cidade inteligente apresentados por Kitchin possuem sérios problemas. Inicialmente, os dados produzidos e coletados em uma cidade inteligente não podem ser acessíveis a todos. Basta citar os casos de tratamento de dados pessoais sensíveis, nos quais as restrições de acesso são fundamentais e inevitáveis, e as informações protegidas pela Lei de Acesso à Informação (LAI), que envolvem a segurança da sociedade e do Estado, sendo classificadas como ultrassecretas, secretas ou reservadas[47].

Ademais, a cidade inteligente é um campo fértil para o tratamento de dados enviesado, que prejudica grupos de pessoas por suas características pessoais, tais como, etnia, gênero, religião e ideologia política. Prevendo o risco da existência de tratamento de dados indevido pelo Estado, a Lei Geral de Proteção de Dados Brasileira regulou um capítulo apenas direcionado ao Poder Público.

Kichin também não leva em consideração a limitação da própria tecnologia em processar dados inúteis ou equivocados. Esse problema, além de prejudicar a prestação de serviços da cidade, também contraria a ideia do autor de processar dados totalmente neutros.

---

[46]KITCHIN, Rob, **The Real-Time City? Big Data and Smart Urbanism** July 3, 2013. GeoJournal 79(1):1-14, 2014, Available at SSRN: https://ssrn.com/abstract=2289141 or http://dx.doi.org/10.2139/ssrn.2289141 2 - 4 p.

[47] "Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada. § 1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no **caput,** vigoram a partir da data de sua produção e são os seguintes: I - ultrassecreta: 25 (vinte e cinco) anos; II - secreta: 15 (quinze) anos; e III - reservada: 5 (cinco) anos." Lei 10.257/2001**. Estatuto da Cidade.**

Estes e outros fatores, que também serão abordados neste trabalho, mostram que a regulamentação e a fiscalização da coleta e do uso dos dados são essenciais para o sucesso de uma cidade inteligente. Porém, este trabalho defende que o controle estatal, embora fundamental, deve ser exercido com parcimônia, incentivando à inovação tecnológica responsável e o desenvolvimento econômico.

Por fim, a ausência de termos que remetem aos direitos do cidadão, como a privacidade e a transparência no tratamento dos dados, evidencia a incompletude dos conceitos de cidade inteligente abordados por Rob Kitchin. O próprio autor assevera que os dados são essenciais para a cidade inteligente, mas, esquece que as operações devem assegurar os direitos e as garantias dos titulares dos dados.

No Brasil, atualmente, tramita, na Câmara dos Deputados, o projeto de lei de nº 976/2021[48], que traz a seguinte definição de cidade inteligente:

> *Art. 2º Para os efeitos desta Lei, entende-se por: I – cidade inteligente: espaço urbano orientado para o investimento em capital humano e social, o desenvolvimento econômico sustentável e o uso de tecnologias disponíveis para aprimorar e interconectar os serviços e a infraestrutura das cidades, de modo inclusivo, participativo, transparente e inovador, com foco na elevação da qualidade de vida e do bem estar dos cidadãos.*

Inicialmente, evidencia-se a influência da doutrina europeia sob o conceito brasileiro de cidade inteligente, pois ambos colocam o bem-estar do cidadão como o objetivo principal da implantação da tecnologia *smart city*, além de destacarem o desenvolvimento econômico sustentável. Todavia, na definição brasileira não há menção sobre o meio ambiente e as futuras gerações, o que denota uma incompletude do conceito em relação ao entendimento europeu.

Um ponto positivo do conceito contido no PL nº 976/2021 é o uso da expressão *espaço urbano*, excluindo o uso da tecnologia *smart city* no ambiente rural. Entende-se que tal medida foi acertada, pois assim é possível distinguir a cidade inteligente da tecnologia *smart city,* que pode ser inserida tanto na cidade como no campo.

Apesar de o objetivo central do conceito de cidade inteligente do projeto de lei estar em consonância com o Direito Urbanístico, o PL não menciona termos importantes como a cooperação entre os elementos da cidade, a participação popular e o planejamento. Ademais,

[48]CAMARA DOS DEPUTADOS. Projeto de lei 976.2021. **Política Nacional de Cidades Inteligentes**. Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449

nota-se a ausência dos dados e suas regras de tratamento, elementos basilares da cidade inteligente, como já foi destacado.

Conforme dito no início deste tópico, o significado de cidade inteligente deve abranger o maior número de fatores possíveis devido a variedade de elementos de uma cidade. Deste modo, este trabalho procura conferir a devida importância a cada elemento encontrado na pesquisa.

Define-se cidade inteligente como uma área *geográfica circunscrita*, preenchida por uma *infraestrutura urbana sustentável* e *habitada por uma aglomeração humana permanente*, que possui *atividades* de desenvolvimento urbano, tecnológico, cultural, econômico, social e ambiental, potencializadas tanto pela inserção eficiente de bens e serviços urbanos tecnológicos como pelo aprimoramento do indivíduo e das organizações públicas e privadas sobre a tecnologia, e *protegidas, planejadas e organizadas* pela administração pública, em cooperação com os demais setores da sociedade, com os *objetivos principais* de garantir o bem estar do cidadão, das gerações futuras e a preservação do meio ambiente, observadas a proteção dos dados pessoais, a privacidade, a segurança da informação, a inclusão social e os demais valores juridicamente protegidos.

1.2. Peculiaridades em cidade inteligente

Apesar de não haver um consenso sobre o significado de cidade inteligente, é inegável que todos os conceitos possuem um ponto em comum, que é o desenvolvimento do ambiente urbano por meio de inovação tecnológica. É através desta ideia que várias organizações estabeleceram rankings para avaliar o quão uma cidade é "inteligente"[49].

Geralmente, o critério utilizado para diferenciar uma cidade tradicional de uma cidade inteligente é o desenvolvimento de setores como mobilidade, saúde e segurança, através da tecnologia. Desse modo, nada melhor do que exemplos de desenvolvimento urbano por setor, classificados como "inteligentes", para diferenciá-los de uma cidade tradicional.

[49]ECONOMIST IMPACAT. **digital cities index** 2022. Disponível em: https://impact.economist.com/projects/digital-cities/2022-executive-summary/?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=19495686130&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=CjwKCAiAwomeBhBWEiwAM43YIF84K7JDoD_XaHdKyRl91Mk2VXqHTrDaLX_7yLtARAJ77npYvMjMARoCGaAQAvD_BwE&gclsrc=aw.ds Acesso em 01/02/2023; RANKING CONNECTED SMART CITIES. **Ranking Connected Smart Cities.** *2022* Disponível em: https://ranking.connectedsmartcities.com.br/

A seguir, serão analisadas as cidades inteligentes situadas na União Europeia (Espanha, Portugal, Noruega e Finlândia), no Reino Unido, nos EUA, em Singapura e na Austrália, respectivamente. Os critérios de escolha dessas regiões foram os seguintes: O avanço da tecnologia em ambiente urbano nos casos dos EUA, Austrália, Singapura, Reino Unido e União Europeia; o desenvolvimento normativo de proteção de dados no caso do Reino Unido e da União Europeia; a similaridade entre os ordenamento jurídicos de proteção de dados nacional e o da União Europeia; os problemas atuais enfrentados na União Europeia relacionados à proteção de dados no ambiente urbano que provavelmente serão encarados no Brasil e; a diferença de entendimento sobre os direitos à privacidade e à proteção de dados pessoais entre a União Europeia e os Estados Unidos.

Ao final deste tópico, estuda um exemplo de implantação de *smart city* na cidade de São Paulo. O objetivo é verificar o estágio de desenvolvimento dessa implantação para, no último capítulo deste trabalho, apontar medidas internacionais de proteção de dados que podem ser aproveitadas no território nacional.

Na União Europeia, especificamente em Barcelona, Espanha, foi criado o programa Laboratório de Mobilidade Urbana, que é um resultado de uma parceria público-privada entre o governo municipal, *startups*, empresas e universidades. Seu objetivo é desenvolver soluções de mobilidade urbana inovadoras para otimizar os itinerários das frotas veiculares, reduzir acidentes de trânsito e diminuir a poluição das zonas urbanas[50].

A prefeitura de Barcelona realiza a coleta de dados e de informações captadas pela infraestrutura da cidade como redes e sensores instalados em ônibus e semáforos. Todos os participantes que estão cadastrados no programa podem usufruir de um espaço público, delimitado pela prefeitura, para testar projetos de inovação em ambientes reais.

O convênio também inclui suporte de profissionais especializados em áreas jurídicas, técnicas e operacionais para avaliar a adequação dos projetos com o GDPR[51]. O programa ainda conta com um escritório especializado em *big data*[52] e a criação de uma plataforma de dados conjunta para que todos possam ter acesso uniforme aos dados coletados.

---

[50] BARCELONA. **Agreement to drive the Mobility of the future**. 27.06.2022. Info Barcelona. Disponível em: https://www.barcelona.cat/infobarcelona/en/tema/smart-city/agreement-to-drive-the-mobility-of-the-future_1190154.html

[51] O *General Data Protection Regulation* (GDPR) é o Regulamento Europeu de Proteção de Dados (UE 2016/679), atualmente a legislação mais influente do mundo nesse assunto.

[52] O termo *big data* será definido em tópico específico.

Um dos projetos do programa é o DTG 3.0[53] (*Dirección General de Tráfico*) que tem como objetivo o desenvolvimento de uma plataforma de dados aberta que interliga os interessados em informações sobre o transporte terrestre, como, os fabricantes de veículos, prestadores de serviços de localização e GPS, aplicativos, câmaras municipais, plataformas de transporte público, sistemas de gestão e frotas e prestadores de serviços de assistência rodoviária[54]. Os dados são coletados por meio de sensores instalados em veículos e sensores da prefeitura.

Os objetivos do DTG 3.0 são coletar informações importantes para potencializar a prestação dos diversos serviços de mobilidade urbana como a melhoria das condições das pistas, o desempenho dos veículos e dos aplicativos móveis e o gerenciamento do tráfego, além de informar os cidadãos sobre a situação em tempo real das vias rodoviárias, como, a realização de eventos, a ocorrência de acidentes, o estado da pista (escorregadia, chuva forte, buraco, etc), as informações dos semáforos, do centro de controle de tráfego da cidade e de vagas nas ruas e em estacionamentos próximos.

Outro projeto em desenvolvimento é o *Autonomous Ready Flota Segura* 3000[55], que prevê a instalação de sistemas de visão artificial (ADAS)[56] em frotas de viaturas particulares. Por fim, cita-se a implantação de melhorias na linha de Ônibus H12, transformando-a em um serviço elétrico que possui conectividade e habilitadores automáticos com *big data* e inteligência artificial.

O MobiCascais[57] é um programa sustentável de mobilidade urbana situado em Cascais, Portugal, e consiste em uma plataforma integradora de vários operadores de serviços de transporte, rede de infraestruturas e equipamentos como ônibus, aluguel de bicicletas e trotinetes elétricas, pagamento de faixa azul e estacionamentos, rede de carregamento de carros

---

[53]DTG. **Qué es DTG 3.0.** Disponível em*: https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/dgt-3.0/*

[54]DTG. **Qué es DTG 3.0.** Disponível em: https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/dgt-3.0/

[55]AUTONOMOUS READY. **El caso Barcelona**. Disponível em: https://autonomousready.org/caso-barcelona/

[56]ADAS são as iniciais de *Advanced Driver Assistance Systems*, ou Sistemas Avançados de Assistência ao Condutor. É um conjunto de funções instaladas no automóvel para aumentar a segurança da condução, reduzindo o risco de colisão. As câmaras instaladas no veículo detectam as distâncias entre o carro e os obstáculos e enviam sinais para o sistema do carro, que ajusta a condução ou avisa o condutor para ajustá-la. TEXAS INSTRUMENTS. **Advanced driver assistance system*s* (ADAS). Driving autonomy forward**. Disponível em < https://www.ti.com/applications/automotive/adas/overview.html?utm_source=google&utm_medium=cpc&utm_campaign=ti-null-null-58700008333137805_dynamicapplications_automotive_adas-cpc-pp-google-wwe_int&utm_term=&ds_k=DYNAMIC+SEARCH+ADS&DCM=yes&gclid=Cj0KCQjwi7GnBhDXARIsAFLvH4nWhb2ILO7z_FMf6iyEe8awIRNQQGZAcOjuaMUMC8TPmxXmQmm_QscaAgKLEALw_wcB&gclsrc=aw.ds>

[57] MOBICASCAIS. **App MobiCascais***.* Disponível em https://mobi.cascais.pt/

elétricos, pontos gratuitos de *wi-fi* e trajeto para autocarros. Desde setembro de 2019, este programa já oferece uma rota específica para autocarros que será ampliada em breve[58].

Além disso, o aplicativo busca incentivar os cidadãos a ter um comportamento positivo com relação ao cuidado com o meio ambiente. Quanto melhor for o seu comportamento, mais pontos o cidadão ganha no aplicativo, podendo trocá-los por diversos benefícios[59].

The European Institute for Innovation through Health Data criou um ecossistema de governança de dados de saúde abrangente, do qual promove padrões de interoperabilidade para conectar os bancos de dados dos sistemas de Registro Eletrônico de Saúde com plataformas de pesquisa europeias.[60] Os objetivos são reutilizar os dados rotineiros de saúde para pesquisa e melhoria do setor, por meio de tecnologias como o *big data* e a inteligência artificial, conectar todas as partes interessadas em dados de saúde e impulsionar um ecossistema colaborativo para o desenvolvimento da área.

O programa de governança de dados de saúde europeu é sustentado por quatro pilares que são: coletar dados de boa qualidade; desenvolver softwares cada vez mais confiáveis; promover o compartilhamento de dados entre os interessados e; proteger os dados pessoais.

O *FutureBuilt* é um programa de parceria público-privada que envolve seis municípios da região de Oslo, na Noruega, alguns órgãos do governo, como o Escritório Nacional de Tecnologia, e empresas privadas. O programa busca o desenvolvimento urbano favorável ao clima e a melhoria da qualidade de vida dos cidadãos. Até novembro de 2022, o *FutureBuilt* possuía 71 projetos piloto, públicos e comercias, envolvendo bairros, moradias, escolas, jardins de infância, prédios comerciais, centros culturais e projetos de ciclismo[61].

Um deles é o *Landbrukskvartalet*[62] que visa criar uma vida urbana autossustentável. Apelidada de bairro agrícola, entre os seus objetivos estão a criação de soluções inteligentes de uso e produção de energia ao nível de bairro por meio de micro redes de energia, que permite a troca de energia entre edifícios, a distribuição do excesso de calor e a redução de picos de carga

---

[58]MOBICASCAIS. **Serviços mobi. Veículos autônomos**. Disponível em https://mobi.cascais.pt/servicos/veiculoautonomo

[59] CRÓ, Isabel, ROEGIERS, Tristan Castro. **Data Protection in the Smart City Of Lisbon**. Flanders, Investment & Trade – Lisbon. 2021 Disponível em: https://www.flandersinvestmentandtrade.com/export/sites/trade/files/market_studies/2021-Portugal-Data%20protection%20in%20the%20smart%20city%20of%20Lisbon-Website_2.pdf 30 p.

[60]HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality**. *Disponível em* https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality

[61]FUTUREBUILT. **What tis FutureBuilt**. Disponível em: https://www.futurebuilt.no/English.

[62]FUTUREBUILT. **Landbrukskvartalet, Oslo.** Disponível em: https://www.futurebuilt.no/English/Pilot-projects?municipal%5B%5D=oslo&function%5B%5D=infrastructure&function%5B%5D=neighbourhoods#!/English/Pilot-projects/Landbrukskvartalet-Oslo

através do armazenamento de energia. A maior parte da energia consumida será produzida por fontes locais.

Além disso, o *Landbrukskvartalet* objetiva desenvolver um espaço verde na cidade, através da utilização de infraestrutura agrícola nos telhados dos edifícios. A proposta, que vai muito além da estética, é promover a produção de alimentos de acordo com as necessidades dos negócios situados no edifício.

O programa ainda conta com o incentivo de compartilhamento de bicicleta para diminuir o uso de veículos automotivos. Nesse aspecto, estuda-se o *Oslo Bysykkel*[63], um aplicativo de compartilhamento de bicicletas que ajuda o cidadão a encontrar e desbloquear bicicletas que estão situadas em 253 estações ao redor de Oslo.

Este aplicativo fornece assinatura mensal ou passes, diário ou único, sendo esse último com permissão de uso de 60 minutos. Após a utilização, o usuário deve deixar a bicicleta em uma das estações espalhadas pela cidade.

Na cidade de Tampere, Finlândia, desenvolve-se o *Smart Urban Security and Event Resilience* (SURE)[64], um projeto de segurança urbana inteligente e de resiliência de eventos[65] que busca oferecer às empresas locais oportunidades para desenvolver e testar as suas inovações, serviços e produtos de segurança urbana em conjunto com o governo. As empresas possuem acesso às áreas urbanas para testar os seus produtos e à infraestrutura tecnológica pública em Tampere para desenvolvê-los.

O SURE propõe apresentar uma solução de segurança urbana por meio de uma plataforma baseada em IoT, que capta informações de pessoas e de fluxos de tráfegos, e de um sistema de IA que identifica comportamentos. Esse sistema também utiliza outros elementos da estrutura urbana, como iluminação pública[66], em prol da segurança. O projeto foi testado com sucesso algumas vezes, sendo um deles no campeonato mundial de Hóquei no Gelo de 2022, realizado em Tempere[67].

---

[63] OSLO CITY BIKE. **Good for you, good for Oslo!** Disponível em: https://oslobysykkel.no/en

[64] TAMPERE. **SURE! Tampere. New ways to keep you secure**. Disponível em: https://suretampere.fi/

[65]Resiliência de Eventos é um método de desenvolvimento de soluções tecnológicas para problemas relacionados à eventos urbanos. No caso do SURE, é aprimorada a tecnologia de segurança urbana integrada, por meio de simulações conjuntas para a cooperação e coordenação entre autoridades urbanas e de segurança, socorristas e organizadores de eventos. **SURE! Tempere. Smart Urban Security and Event Resilience – SURE**. Disponível em: https://suretampere.fi/what-is-sure/#:~:text=Smart%20Urban%20Security%20and%20Event%20Resilience%20%2D%20SURE&text=The%20project%20aims%20to%20increase,will%20be%20utilized%20and%20integrated. Acesso em 28/08/2023

[66] NORDIC SMART CITY CITY NETWORK. **Smart city update from Tampere: Improving health care and Heighteninig public safety**. Disponível em: https://nscn.eu/cityupdate/Tampere/healthandsafety

[67] TAMPERE. **Urban security model developed in Tampere scales up in other European cities**. 06/07/2022. Disponível em: https://suretampere.fi/urban-security-model-developed-in-tampere-scales-up-in-other-european-cities/

Em 2018, a prefeitura da cidade de Londres lançou o projeto *London Together* de implantação da tecnologia de cidade inteligente nos serviços públicos até 2050. Em 2021, esta prefeitura publicou um relatório sobre os avanços conquistados nos três primeiros anos e os planos da cidade para o futuro[68].

Na vanguarda da implantação de tecnologia *smart city*, Londres possui uma plataforma de dados desde 2010. O *London Datastore*[69] é o portal padrão de compartilhamento de dados gratuito e aberto para qualquer pessoa. Seu objetivo é coletar, processar, organizar e divulgar os dados da cidade de Londres para auxiliar o desenvolvimento dos serviços públicos e promover a criação de novos produtos e serviços.

O *London Datastore* fornece dados atuais sobre as questões mais importantes da cidade como o índice de emprego, desempenho dos transportes públicos, qualidade do ambiente, índice de criminalidade, habitação, tamanho populacional e saúde. Neste último exemplo, a plataforma acompanha os costumes dos cidadãos londrinos verificando a quantidade de bebida alcoólica consumida e a obesidade infantil[70].

Esta plataforma evoluiu e hoje também é utilizada para a venda e o compartilhamento de dados não abertos e privados entre organizações[71]. No *London Datastore* é possível criar conjuntos de dados, fazer upload de vários arquivos, fornecer descrições dos dados (metadados) e fazer atualizações dos dados a qualquer momento, sem que outros possam alterá-los. Além disso, o seu sistema de armazenamento de dados está localizado em um *datacenter* no Reino Unido, o que é um grande trunfo para a proteção dos dados pessoais dos londrinos.

Como se não bastasse, a plataforma também possui outros serviços de dados para situações específicas. O *spend data* é o compartilhamento de dados coletados em cartões da *Mastercard* para identificar mudanças, ao longo do tempo, nos padrões de gastos dos londrinos. Para ter acesso a esses dados, além da necessidade de ter uma parceria com a prefeitura de Londres, o interessado deve pagar um valor financeiro pelo serviço[72].

---

[68]BLACKWELL, Theo; THOMSON, Julia. **Smart London Together Roadmap 2018-21.Report back to Mayor of London .** October 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.london.gov.uk/sites/default/files/slt_roadmap_summary_paper_for_2021.pdf

[69]MAYOR OF LONDON. **London Datastore.** Disponível em:https://data.london.gov.uk/?_gl=1%2a17r8k54%2a_ga%2aNDA4NzczMTUuMTY3ODg3NjIzNA..%2a_ga_PY4SWZN1RJ%2aMTY3OTM4OTEwMy4xLjAuMTY3OTM4OTEwMy42MC4wLjA. Acesso em 21/03/2023

[70]MAYOR OF LONDON. **London Datastore**. Disponível em: https://data.london.gov.uk/?_gl=1%2a17r8k54%2a_ga%2aNDA4NzczMTUuMTY3ODg3NjIzNA..%2a_ga_PY4SWZN1RJ%2aMTY3OTM4OTEwMy4xLjAuMTY3OTM4OTEwMy42MC4wLjA. Acesso em 21/03/2023

[71]MAYOR OF LONDON. **The London Datastore offer**. https://data.london.gov.uk/borough-partnership/the-london-datastore-offer/ Acesso em 22/03/2023

[72]MAYOR OF LONDON. **High Street Data Service and Partnership**. Disponível em: https://data.london.gov.uk/high-street-data-service/ Acesso em 21/03/2023

Outro exemplo de serviço específico da plataforma londrina é o *footfall data,* que compartilha dados anonimizados sobre o número de pessoas que moram em determinada área. Para isso, os dados identificam três grupos, sendo eles os residentes, os trabalhadores e os visitantes daquela região[73]. Da mesma forma que o *spend data,* o *footfall data* apenas é acessível aos parceiros de Londres que pagam pela informação.

Nos Estados Unidos, desenvolve-se o *Array of Things* (AoT)[74], projeto que conta com a participação de cientistas, governo federal, algumas prefeituras, universidades, indústria e comunidades locais. O AoT é um sistema de medição urbana que possui "nós" modulares e programáveis com sensores e capacidade de computação para coleta e análise interna de dados como, por exemplo, contagem de número de veículos em um cruzamento. Este sistema exclui, depois da contagem, os dados da imagem captada ao em vez de enviá-los para um local de armazenamento centralizado (*datacenter*).

O *Array of Things* desenvolveu, na cidade de Chicago, instalações de dispositivos que coletam dados, quarteirão a quarteirão, sobre a qualidade do ar, os níveis de ruído, de tráfego de veículos e de pedestres[75]. Alguns exemplos de uso do *Array of Things* são sensores para medir e economizar a luz pública, escurecendo automaticamente as ruas em períodos não necessários; sensores de água instalados em rios para monitorar inundações e; software instalado em câmeras, que auxilia na detecção de crimes como determinar a origem de um tiro.

O projeto utiliza uma plataforma aberta de detecção inteligente e computação de borda[76] chamada *Waggle*[77]. Este sistema consiste em aplicativos de computação de ponta que processam dados, como, leituras de sensores, imagens de câmeras e gravação de áudio.

Esses aplicativos de borda produzem seus próprios dados e carregam os resultados em um banco de dados em nuvem. Inclusive, no próprio site do *Waggle* há recomendações sobre como criar o seu próprio aplicativo[78].

---

[73]MAYOR OF LONDON. **High Street Data Service and Partnership.** Disponível em: https://data.london.gov.uk/high-street-data-service/ Acesso em 21/03/2023

[74]ARRAY OF THINGS. **Sage**. *Disponível em:* https://arrayofthings.github.io/

[75]MADHANI. AAMER. **Chicago begins Building "fitness tracker" to check its vitals**. 29/08/2016. Usa Today. Disponível em: https://eu.usatoday.com/story/news/2016/08/29/chicago-begins-building-fitness-tracker-check-its-vitals/89434620/

[76]"Edge computing describes the use of computing resources (including data storage and processing) located close to the devices which generate the data, Rather than relaying this data to a remote cloud computer to perform computations. It issuited to applications that require quick computation and use large volumes of data, which would require high bandwidth for transfer to the cloud. It may also offer some privacy benefits as more data can be processed locally rather than being sent to a cloud. However, the distributed nature of edge computing, and the need for many individual devices to connect and interact, poses a number of unique challenges to its widespread adoption". UK PARLIAMENT. **Resarch Briefing, Smart Cities.** 22/09/2021.

[77]WAGGLE AI. ***Scientific AI at the edge***. Disponível em: https://wa8.gl/

[78]WAGGLE. **Access Waggle sensors**. Disponível em: https://docs.waggle-edge.ai/docs/tutorials/access-waggle-sensors

Qualquer colaborador pode instalar um sensor no *edge computer* do *Waggle* e usufruir tanto da sua tecnologia como da sua base de dados, desde que respeite a Política de Privacidade do AoT[79]. Porém, apenas esta medida não é capaz de sanar todas as preocupações sobre os riscos à proteção dos dados pessoais que serão analisados no decorrer deste trabalho.

Alguns aplicativos desta tecnologia estão em destaque como o *Sage*[80], que são redes de sensores inteligentes e distribuídos que coletam dados para auxiliar os cientistas sobre os impactos da urbanização global, os desastres naturais, como inundações e incêndios florestais, e mudanças climáticas nos ecossistemas naturais e nas infraestruturas das cidades.

Em 2014, no sudeste asiático, o governo de Singapura criou o *Singapore's Smart Nation*, um programa de implantação de tecnologia de cidade inteligente em diversos setores públicos, como, mobilidade, e-governança[81] e saúde. Além do governo local, empresas e cidadãos participam do seu desenvolvimento[82].

Esse projeto implantou tecnologia assistiva e robótica para melhorar a saúde dos cidadãos. O *RoboCoach Xian* é uma máquina que ensina exercícios físicos a idosos e crianças, além de oferecer terapia física e cognitiva para pacientes que sofreram AVC ou que estão com Alzheimer ou Parkinson[83]. O *RoboCoach Xian* está sendo preparado para ajudar deficientes visuais a desenvolver a sua comunicação.

---

[79]ARRAY OF THINGS. **Array of Things Governance & Privacy Policies**. Disponível em: https://arrayofthings.github.io/privacypolicy.html

[80]SAGE. **AI @ the edge for**. Disponível em: https://sagecontinuum.org/

[81]Em inglês, *eletronic government* (EGov), é a utilização estratégica da Tecnologia da Informação pelo Poder Público para fornecer serviços externos de acesso fácil a informações e serviços governamentais para cidadãos e empresas; aumentar a qualidade dos serviços, tornando-os rápidos, eficientes e íntegros; conceder aos cidadãos a oportunidade de participar de assuntos de interesse público. Também se usa a TI para serviços públicos internos como o autoatendimento. GRÖNLUND, Åke. **Electronic government: design, applications & management**. Hershey: Idea Group Publishing, 2002. 23-50 p.

[82]SINGAPURE. **Digital Readiness Blueprint**. Disponível em: https://www.mci.gov.sg/-/media/MciCorp/Doc/MCI_Blueprint-Report_FINAL.ashx

[83]SINGAPURE. **Smart Nation. Assistive Technology and Robotics In Healthcare. Improve Healthcare with Tech.** Disponível em*:* https://www.smartnation.gov.sg/initiatives/health/assistive-techonology-robotics

Figura 1. Imagem do *RoboCoach Xian*[84]

A *SG Enable*, agência de tecnologia integrante da *Singapore's Smart Nation* voltada para o desenvolvimento de programas para os deficientes, inaugurou a *Tech Able*[85], que é um espaço integrado de tecnologia assistiva que fornece um serviço de avaliação de dispositivos auxiliares. O seu objetivo é ajudar os deficientes a descobrir dispositivos que irão capacitá-los para o mercado de trabalho ou auxiliá-los nas atividades do dia a dia.

O *Switching on Darwin*[86]é um projeto de cidade inteligente lançado na cidade de Darwin, situada no norte da Austrália, que objetiva reduzir a criminalidade através de um sistema sofisticado de iluminação pública. Além da instalação de luzes LED, o projeto criou colunas "*smarts"* que usam câmeras para detectar atividades criminosas. Este sistema de iluminação também é equipado por sistemas com sensores de som que captam gritos de socorro e notificam imediatamente as autoridades locais.

[84]SINGAPURE. *Smart Nation*. *Assistive Technology and Robotics In Healthcare.* https://www.smartnation.gov.sg/initiatives/health/assistive-techonology-robotics
[85]SINGAPURE. **Smart Nation. Apps for you**. Disponível em https://www.smartnation.gov.sg/community/apps-for-you/
[86]ECO RENEWABLE ENERGY. **Transforming Cities, Empowering Communities: 7 Smart Cities Australia Projects.** Disponível em: https://www.ecorenewableenergy.com.au/articles/building-smart-cities-australia-6-notable-projects/

Além disso, o CCTV (*Closed-circuit Television*) instalado em Darwin é utilizado como uma ferramenta para gerenciar o comportamento antissocial, coletar dados sobre o movimento de veículos e de pedestres na cidade e auxiliar o planejamento urbano.

Segundo a prefeitura de Darwin, o sistema de CCTV não inclui reconhecimento facial, o áudio captado não é gravado e a filmagem não está disponível para o público. Os dados coletados são anonimizados e se referem a informações estatísticas como o número de pessoas em determinadas áreas, o sentido do deslocamento das pessoas, as rotas mais utilizadas e os movimentos dos veículos[87].

A cidade de Adelaide, também na Austrália, apresenta avanços significativos na implantação de tecnologia de cidade inteligente[88]. Um exemplo é a lixeira *Clean Cube* instalada pela prefeitura em parceria com a empresa australiana *Smart City Solutions*.

Uma lixeira normal é inserida em uma estrutura cúbica, chamada *Clean Cube*, que possui um sistema de coleta e processamento de dados baseado em *cloud*[89]. O sensor instalado no cubo fornece informações em tempo real sobre a quantidade de lixo no compartimento.

A nova tecnologia ajuda a evitar que o lixo transborde pela calçada, além de potencializar o serviço de coleta, uma vez que a lixeira só é esvaziada quando necessário. A estrutura também possui um compactador de lixo que aumenta em até oito vezes a capacidade da lixeira[90].

Na cidade de São Paulo/SP é desenvolvido o *Smart Sampa*, programa de videomonitoramento urbano[91]. Em agosto de 2023, iniciou-se a instalação de 20 mil câmeras inteligentes com tecnologia de biometria facial que integrará diversos serviços públicos.

---

[87]CITY OF DARWIN. **Switching on Darwin.** Disponível em: https://www.darwin.nt.gov.au/transforming-darwin/innovation/switching-on-darwin

[88]CITY OF ADELAIDE. **Smart city Adelaide**. Disponível em*:* https://www.cityofadelaide.com.au/about-adelaide/smart-city-adelaide/

[89] "Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand. Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers*"*. HON, W. Kuan and MILLARD, Christopher and Walden, Ian, **The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated?** The Cloud of Unknowing, Part 1 (March 10, 2011). International Data Privacy Law (2011) 1 (4): 211-228, Queen Mary School of Law Legal Studies Research Paper No. 75/2011, Available at SSRN: https://ssrn.com/abstract=1783577 or http://dx.doi.org/10.2139/ssrn.1783577 acesso em 24/04/2023

[90]CITY OF ADELAIDE. **Smart Bins to Keep Adelaide's Streets Cleaner**. *Disponível em:* https://www.cityofadelaide.com.au/media-centre/smart-bins-to-keep-adelaides-streets-cleaner/

[91]PREFEITURA DE SÃO PAULO. **Prefeito assina contrato para o início do Smart Sampa, o maior programa de videomonitoramento da cidade com até 40 mil câmeras.** 07/08/2023. https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2

O programa promete oferecer maior segurança aos cidadãos, além de aumentar a agilidade na prestação de serviços públicos como SAMU, Metrô e o SPTrans. A integração dos dados entre órgãos públicos ocorrerá através de uma central inteligente de monitoramento.

Segundo a prefeitura de São Paulo, existe uma atenção especial com a proteção dos dados pessoais do cidadão. A Secretaria Municipal de Segurança Urbana da cidade criou políticas de segurança da informação, de segurança cibernética e de integridade ética, além de um relatório sobre o impacto da proteção dos dados pessoais[92].

Para facilitar a comparação entre os exemplos de tecnologia de cidade inteligente estudados neste tópico, criou-se a tabela "*smart city.* Ela auxilia na identificação do setor de atuação de cada programa ou produto, a sua finalidade e as principais tecnologias utilizadas.

TABELA "SMART" CITY				
Programa ou produto	**Origem**	**Setor de atuação**	**Finalidade**	**Principais Tecnologias utilizadas**
Array of Things (AoT)/*Waggle/ Sage*	Estados Unidos	Pesquisa, saúde, segurança pública e meio ambiente	Sistema de medição urbana para coletar diversos tipos de dados e utiliza-los para pesquisa, monitoramento, controle e economia de recursos.	Internet das Coisas, câmeras de áudio e vídeo, *edge computer* e *cloud*
Clean Cube	Adelaide/ Austrália	Limpeza pública	Aumentar a capacidade da lixeira e potencializar o serviço de coleta.	Sensor e *Cloud*
European Institute for Innovation through Health Data	União Europeia	Governança de dados e Saúde	Auxiliar pesquisas e desenvolver tecnologia para a saúde e para a governança de dados	*Big Data*, Inteligência Artificial

[92]PREFEITURA DE SÃO PAULO. **Prefeito assina contrato para o início do Smart Sampa, o maior programa de videomonitoramento da cidade com até 40 mil câmeras.** 07/08/2023. Disponível em: https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2

FutureBuilt /Landbrukskvartalet	Oslo/Noruega	Energia e meio ambiente	Buscar soluções econômicas e eficazes para o uso e produção de energia a nível de bairro. Desenvolver infraestrutura verde nos edifícios	Sensores e sistemas de integração de imóveis urbanos
London Together /London Datastore	Londres/ Reino Unido	Governança de dados	Compartilhar dados da cidade de Londres para desenvolver políticas públicas e inovar serviços e produtos	*Big data*, sensores de IoT
MobiCascais	Cascais/ Portugal	Mobilidade Urbana	Facilitar o acesso ao transporte público, aprimorar os serviços de transporte e incentivar a mobilidade sustentável	Plataforma digital, sensores de IoT e aplicativos de mobilidade urbana
Oslo Bysykkel	Oslo/Noruega	Mobilidade urbana e meio ambiente	Compartilhar bicicletas para diminuir o uso de veículo automotivo	Plataforma digital e aplicativos de mobilidade urbana
Singapore's Smart Nation/ RoboCoach Xian	Singapura	Saúde	Ensinar exercícios físicos a idosos e crianças. Oferecer terapia física e cognitiva para pacientes com Alzheimer, Parkinson e AVC	Tecnologia assistiva e robótica

Smart Sampa	São Paulo/ Brasil	Segurança urbana	Aumentar a segurança pública e a eficiência de outros serviços públicos	Câmeras com reconhecimento facial e plataforma de compartilhamento de dados
Smart Urban Security and Event Resilience (SURE)	Tampere/ Finlândia	Segurança Pública	Desenvolver produtos e serviços de tecnologia para a segurança	Internet das Coisas, Inteligência Artificial
Switching on Darwin	Darwin/ Austrália	Segurança e iluminação Pública	Aumentar a segurança através de um sistema de iluminação pública e câmeras de som e imagem	CCTV, LED e sensores de som
Urban Mobility Lab/ Dirección General de Tráfico	Barcelona/ES	Mobilidade Urbana	Criar plataforma aberta de dados de transporte terrestre para potencializar a prestação de serviços e aprimorar veículos	sensores de IoT, câmeras e plataforma digital de compartilhamento de dados.
Urban Mobility Lab/Ready Flota Segura 3000	Barcelona/ Espanha	Mobilidade Urbana	Aprimorar a segurança da condução veicular	Advanced Driver Assistance Systems -ADAS

Tabela 1. Autoria própria

1.3. Desafios identificados para a Proteção de Dados Pessoais em *smart city*

Este tópico apresenta os desafios para a proteção de dados pessoais em cidades inteligentes, os quais serão detalhados no próximo capítulo. Sua proposta é identificar tais desafios por meio dos casos concretos anteriormente apresentados, unindo-os à teoria.

Atualmente, não existe legislação específica sobre a tecnologia de cidade inteligente no Brasil. Além do mais, não há sequer uma regra específica no ordenamento jurídico que aborde a proteção de dados pessoais no contexto de cidade inteligente.

Esta ausência legislativa é o primeiro grande desafio à proteção dos dados pessoais, pois obriga os operadores do direito a interpretar e adequar o conjunto normativo existente às

situações específicas de uso de tecnologia em ambientes urbanos, que colocam em risco os direitos e garantias relacionados à proteção dos dados pessoais.

Até o momento, esta realidade não irá mudar, mesmo com a eventual promulgação do projeto de lei 976/2021, que dispõe sobre princípios e diretrizes da Política Nacional de Cidades Inteligentes (PNCI)[93]. Este projeto transfere a responsabilidade normativa da proteção de dados pessoais em cidade inteligente para a Lei Geral de Proteção de Dados (LGPD)[94], que também não possui qualquer dispositivo específico sobre o tema, no contexto de cidade inteligente.

Entretanto é importante destacar que não houve qualquer omissão ou descaso do legislador na confecção da LGPD, já que o objetivo da sua criação sempre foi o de ocupar o status de uma lei geral de proteção de dados pessoais. Portanto, ela não tem a função de normatizar situações específicas como a proteção de dados pessoais em Inteligência Artificial, em Internet das Coisas e em cidade inteligente.

Todavia, a ausência de legislação específica sobre o objeto deste estudo tende a ser problemática, pois a utilização de tecnologias em ambientes urbanos trouxe um novo panorama para o tratamento dos dados pessoais. A começar por tecnologias que possuem características de funcionamento contrárias aos princípios da proteção de dados pessoais.

Um exemplo disso é o *big data,* uma das tecnologias mais utilizadas em cidades inteligentes. Como será analisado em tópico específico, é da natureza do *big data* coletar e processar todos os dados possíveis, o que contraria os princípios da minimização dos dados do GDPR[95] e da necessidade da LGPD[96].

O *data minimization* está contido no princípio da necessidade e consiste no *dever de coletar o mínimo* de dados pessoais possível para a realização de um determinado tratamento

---

[93] "Art. 1º Esta Lei institui a Política Nacional de Cidades Inteligentes (PNCI), com vistas à melhoria da qualidade de vida dos munícipes, e dispõe sobre os princípios e diretrizes que a nortearão, os seus objetivos, as ações a serem realizadas, os recursos alocáveis e dá outras providências". CAMARA DOS DEPUTADOS. Projeto de lei 976/2021. **Política Nacional de Cidades inteligentes**. Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449 Acesso em 27/04/2022

[94] "XIV – Transparência e publicidade de dados e informações, sem prejuízo à privacidade da população e à segurança dos dados; § 2º A observância da privacidade e da segurança de que trata o inciso XIV deverá levar em consideração a necessária garantia da proteção dos dados pessoais e o uso das melhores práticas, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018". CAMARA DOS DEPUTADOS. Projeto de lei 976/2021. **Política Nacional de Cidades inteligentes**. Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449 Acesso em 27/04/2022

[95] "Artigo 5º -Princípios relativos ao tratamento de dados pessoais. Os dados pessoais são: c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados)". GDPR.

[96] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: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"*;* LGPD

de dados. O responsável pelo tratamento deve recolher apenas informações pessoais relevantes e necessárias para atingir a uma finalidade específica[97].

Já o princípio da necessidade, na LGPD, determina a *restrição do uso* dos dados pessoais ao mínimo necessário para atingir a finalidade legítima, em atenção à adequação entre meios e fins, de forma pertinente, proporcional e não excessiva[98]. Assim como no ordenamento europeu, a ANPD desaconselha o tratamento de dados pessoais quando a finalidade almejada pode ser alcançada por meios menos gravosos para os titulares[99].

Outro desafio para a proteção de dados pessoais em cidades inteligentes é a criação de um sistema local de armazenamento e de análise de um volume massivo de dados. Muitas cidades precisam do auxílio de empresas estrangeiras para a prestação desse serviço, pois não dispõem de tecnologia ou de recursos financeiros para criar um sistema desse calibre.

A dependência das cidades perante entidades estrangeiras para armazenar e processar os seus dados constitui sério risco à proteção dos dados pessoais. As entidades estrangeiras terão grande poder sobre os dados dos cidadãos e do governo local, e podem não ter interesse em criar mecanismos de proteção, além de compartilhar esses dados com outras entidades, sejam elas públicas ou privadas. Neste último caso, tem-se até mesmo um risco à segurança nacional.

Além disso, existem as limitações da própria tecnologia em garantir a segurança do armazenamento de grande volume de dados. Um exemplo é a tecnologia *cloud*, amplamente utilizada em cidade inteligente (a exemplo das plataformas digitais, do *Array of Things* e do *clean cube* estudados no tópico anterior) que só em 2022 sofreu várias violações de dados em vários setores que a utilizou para armazenagem.[100]

---

[97]EUROPEAN DATA PROTECTION SUPERVISOR. **Data minimization** disponível em https://edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=Data%20minimization,necessary%20to%20fulfil%20that%20purpose.

[98] MARTINS, Guilherme Magalhães. **A lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a sua principiologia.** Revista dos Tribunais Online. Thomson Reuters, Vol. 1027/2021. p 203 -243. Maio de 2021. 15 p

[99]ANPD. **Guia orientativo de Tratamento de dados pessoais pelo Poder Público**. Versão 2.0. Junho de 2023. Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 25 p.

[100] Vários são o vazamento da dados em nuvem. Vide alguns exemplos: *"*Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket: 'Lives at Stake'*"* Disponível em: https://www.darkreading.com/application-security/cloud-misconfig-exposes-3tb-sensitive-airport-data-amazon-s3-bucket ; "Did Anonymous Carry Out a Cyber Attack on Nestlé? Company Claims Data Leak Was Internal*"* Disponível em: https://www.cpomagazine.com/cyber-security/did-anonymous-carry-out-a-cyber-attack-on-nestle-company-claims-data-leak-was-internal/ *"*Japanese medical online consultation site leaking consumer-submitted images of symptom*"*. Disponível em: https://www.databreaches.net/japanese-medical-online-consultation-site-leaking-consumer-submitted-images-of-symptoms/

Outro problema gerado pelo grande volume de dados é a formação de dados não estruturados[101], situação recorrente em cidades inteligentes. Em linhas gerais, a falta de uma arquitetura compacta e organizada gera maiores custos de armazenamento, além de tornar muito mais difícil a garantia da segurança dos dados pessoais, constante na LGPD[102].

A segurança dos dados pessoais consiste em estabelecer medidas técnicas e administrativas para prevenir situações acidentais ou ilícitas como a destruição, a perda, a difusão dos dados pessoais e para proteger os dados pessoais de acessos não autorizados[103]. Estas medidas devem ser proporcionais aos potenciais riscos e aos direitos fundamentais protegidos.

Outro desafio ocorre quando a análise dos dados não estruturados implica em resultados inúteis, e até mesmo inverídicos, o que vai na contramão dos princípios da qualidade dos dados[104] e da não discriminação[105], além de prejudicar a prestação dos serviços públicos em cidades inteligentes. Estes problemas são ainda mais sérios quando a tecnologia trata de dados pessoais sensíveis.

O próprio *European Institute for Innovation through Health Data,* instituto analisado no tópico anterior, voltado para o desenvolvimento da tecnologia de tratamento e compartilhamento de dados de saúde dos europeus, destaca a importância da qualidade dos dados. Segundo o programa, a clareza e a qualidade dos dados coletados dos pacientes são fundamentais para as tomadas de decisões e inferências clinicas válidas e confiáveis[106].

---

[101] "**Dados não estruturados** são dados que não possuem estrutura ou arquitetura identificável. Isso significa que eles não estão em conformidade com um modelo de dados predefinido e, desta forma, não são adequados para um banco de dados relacional convencional. Não ter uma estrutura facilmente identificável dificulta a leitura por um programa de computador". TIBCO. **O que são Dados não Estruturados?** Disponível em https://www.tibco.com/pt-br/reference-center/what-is-unstructured-data#:~:text=Dados%20n%C3%A3o%20estruturados%20s%C3%A3o%20dados,banco%20de%20dados%20relacional%20convencional.

[102]"Artigo 6º, inciso 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;" Lei 13.709/2018. **Lei Geral de Proteção de dados Pessoais.**

[103]ANPD. **Guia orientativo de Tratamento de dados pessoais pelo Poder Público**. Versão 2.0. Junho de 2023. Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 34 p.

[104] Artigo 6º da LGPD. " 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"

[105] Artigo 6º da LGPD "IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos"

[106]HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality**. *Disponível em* https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality

Já a discriminação pode ocorrer em tecnologias que utilizam algoritmos de inteligência artificial[107], a exemplo do *machine learning*[108], cuja tomada de decisão automatizada pode ser baseada em estatísticas do passado que reproduzem antigos preconceitos.

Outro problema decorrente dos dados não estruturados é a dificuldade em garantir o direito à portabilidade[109], que exige dos responsáveis pelo tratamento a criação de meio de transferência de dados, automática e sem custo, a outro prestador de serviço semelhante, o que pressupõe que os dados já estejam em formato estruturado e interoperável[110]. A falta de padronização do formato dos dados entre os controladores de uma cidade inteligente é um problema, pois algum controlador pode alegar inviabilidade técnica perante o pedido de portabilidade dos dados pessoais do titular.

Esta atitude ilegal do controlador viola o princípio da livre concorrência e o equilíbrio do mercado, pois dificulta ou até impossibilita que o titular dos dados migre para outro prestador de serviço do seu interesse. Sem o direito de portabilidade, é possível que o cidadão tenha

---

[107] "*The first step to properly answer that question is acknowledging that AI is not a single, monolithic concept. On the contrary, AI-based products and services embrace a wide variety of sector-specific applications with different purposes, accuracy, and risks. Indeed, there is no one-size-fits-all definition of AI. (...) No matter the field, the term "artificial intelligence" is misleading because it directly associates algorithmic processes with a simulation of human intelligence. Neuroscientists strongly refuse that kind of association. More than just a terminological problem, the expression artificial intelligence deviates us from what really matters and brings nonsensical questions to the debate. (...) Scientific expressions better than AI would be "analytical computing" or "machine behaviour". However, since "artificial intelligence (AI)" has become the leading term, worldwide, this study will adopt it*. PARENTONI, Leonardo Netto. **What Should We Reasonably Expect From Artificial Intelligence?** Julho de 2022. Disponível em: https://www.researchgate.net/publication/361988480_What_should_we_reasonably_expect_from_artificial_intelligence 4. p

[108]É um ramo da inteligência artificial que envolve o aprendizado a partir de dados, a captação de padrões e a automatização de decisões (SILVA, 2021) DE LIMA, Cíntia Rosa Pereira de. **O impacto social causado pelo uso de algoritmos discriminatórios e a superveniência da LGPD**. 04/11/2022 Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/376497/o-impacto-social-causado-pelo-uso-de-algoritmos-discriminatorios

[109]Art. 18º da LGPD "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: "V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial";

[110] "Como se pode perceber, interoperabilidade é a capacidade de um sistema de se comunicar com outro, de modo harmônico. Para tanto, é necessário que ambos sejam compatíveis e obedeçam a um conjunto mínimo de normas e especificações técnicas (...). Há duas espécies de interoperabilidade: a objetiva e a subjetiva. Aquela se relaciona à utilização de um padrão operacional mínimo que permita *compatibilizar os meios materiais e imateriais* que compõem a infraestrutura, como *softwares*, *hardwares*, cabos, tipo de voltagem, etc. Diz-se *objetiva* por referir-se aos equipamentos utilizados no procedimento e não aos sujeitos que dele participam. Por outro lado, a interoperabilidade *subjetiva* é um conjunto de princípios e regras que incide sobre os sujeitos que, de um modo ou de outro, se relacionam com essa infraestrutura, como os órgãos de fiscalização e execução, os usuários, etc." PARENTONI, Leonardo Netto; OLIVEIRA, Raquel Diniz. **Uma Advertência sobre interoperabilidade e o artigo 154, parágrafo único, do CPC**. Revista Magister de Direito Civil e Processual Civil. Porto Alegre. Magister. Ano IV. Nº 19. 51-73 p. July 2007. Disponível em: https://www.researchgate.net/publication/299802114_Uma_advertencia_sobre_Interoperabilidade_e_o_artigo_154_paragrafo_unico_do_CPC 20 - 22 p.

prejuízos, como, dispêndio de tempo para coletar os dados ou a perda de dados, quando forem irrecuperáveis[111].

O risco à privacidade dos cidadãos também é um dos grandes desafios enfrentados pelos defensores da cidade inteligente. A desconfiança de parte considerável da população na utilização da tecnologia em ambiente público, seja ela controlada pelo Estado ou pela iniciativa privada, vem de uma vigilância velada daquele que detém a tecnologia sob a vida dos cidadãos e o uso indevido dos dados coletados.

Shoshana Zuboff alerta sobre o capitalismo de vigilância, no qual seriam instalados computadores em todos os lugares do ambiente urbano com o propósito de coletar dados além dos limites da consciência individual. Desse modo, o controlador teria ilimitadas informações acerca da vida dos cidadãos[112] e, por consequência, um grande poder sobre eles.

O risco à privacidade é ainda mais evidente quando se trata da instalação de dispositivos que captam áudio e imagens dos cidadãos, conforme mostrado pelo exemplo da Australia. A instalação do sistema CCTV em Darwin foi alvo de críticas do meio acadêmico e da população locais que, além de temerem pelo uso de tecnologia de reconhecimento facial, alegaram que a Avaliação do Impacto de Privacidade só foi realizada depois que o sistema já estava instalado e em operação. [113]

Além do mais, a identificação dos agentes de tratamento[114] e a fiscalização sob as suas atividades podem ser tarefas árduas em cidades inteligentes. A exemplo do *Array of Things*, projeto estadunidense tratado no tópico anterior, a cada dia mais dispositivos de coleta e processamento de dados são instalados nos ambientes urbanos por novas entidades, cada qual com a sua finalidade.

Cada vez mais empresas, entidades governamentais e de pesquisa têm acesso aos bancos de dados das tecnologias de cidade inteligente. Mesmo na Europa, região marcada pela preocupação com os direitos e garantias da proteção dos dados pessoais, constata-se um movimento de inclusão e compartilhamento de informações entre organizações, como são os

---

[111] CRAVO, Daniela Copetti. **Direito à Portabilidade de Dados: Necessidade de Regulação EX ante e EX post.** Tese de Doutorado. Universidade Federal do Rio Grande do Sul. 2018. Porto Alegre. Disponível em: https://lume.ufrgs.br/handle/10183/180184 13 p.

[112]ZUBOFF, Shoshana, **A era do capitalismo de vigilância. A luta por um futuro humano na nova fronteira pelo poder.** 2019. 1º edição. Editora Intrínseca Ltda. 276 p.

[113]ASHTON, Kate. **Darwin Council promises not to use facial recognition technology in new CCTV cameras.** ABC News. 18/08/2019. Disponível em: https://www.abc.net.au/news/2019-08-19/darwin-cctv-facial-recognition-technology-raises-concerns/11425822 Acesso em 06/06/2023

[114] A LGPD define, em seu artigo 5º, inciso IX, agentes de tratamento o controlador e o processador, que são os sujeitos responsáveis pela tomada de decisão do tratamento de dados e pela execução das operações relacionadas ao tratamento.

casos dos exemplos da *European Institute for Innovation through Health Data* na área da saúde, do *DTG* no setor de mobilidade espanhol e do SURE na área da segurança urbana da Finlândia.

Assim, acaba por criar outro problema que é a dificuldade de enquadrar cada entidade controladora nas hipóteses legais de tratamento de dados (coloquialmente conhecidas como "bases legais"). Muitos dos controladores de dados sequer têm o conhecimento do sistema de proteção de dados, muito menos das suas obrigações estabelecidas por esse ordenamento.

Ademais, a cada dia se criam novas funções para a tecnologia no ambiente urbano, o que dificulta o enquadramento legal dessas atividades inovadoras nas hipóteses legais de tratamento de dados pessoais. Acompanhar a evolução tecnológica é um grande desafio para o ordenamento jurídico, que pode não amparar todas as situações concretas envolvendo direito e tecnologia no ambiente urbano.

Além disso, mesmo tendo o conhecimento sobre quem são os controladores de dados em cidades inteligentes e quais são as finalidades legais de cada atividade de tratamento, têm-se os desafios de fiscalização contra o compartilhamento indevido de dados pessoais e o desvio da finalidade de cada operação de tratamento[115]. Nestes casos, depara-se com os problemas de desconhecimento de alguns controladores sobre os ditames legais do tratamento de dados pessoais e com o imenso número de entidades que deveriam ser observadas, especificamente no contexto de cidade inteligente.

Apesar de a lei estabelecer que os próprios controladores exerçam a fiscalização sobre o seu tratamento de dados[116], essa medida, por si só, não resolve o problema para a implantação de tecnologia de cidade inteligente. Neste caso, confiar demasiadamente na boa fé dos controladores pode trazer sérios riscos à proteção dos dados pessoais, pelos diversos fatores citados neste item, como, os riscos à privacidade e à segurança nacional e a negligência dos controladores na tomada de medidas protetivas contra incidentes de segurança[117] envolvendo dados pessoais.

---

[115] Infere-se do artigo 5º, inciso X da LGPD, que operação de tratamento é todo procedimento realizado com dados pessoais tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[116] Esta imposição legal se deve à influência do princípio do *accountability* previsto no artigo 5º, 2 e art. 24º, 1 do GDPR que corresponde ao princípio da "responsabilização e prestação de contas" constante no artigo 6º inciso X da LGPD. O *accountability* pressupõe a boa-fé do controlador, já que determina a demonstração da regularidade de suas operações apenas nos casos em que seja demandado pela ANPD. Para mais informações: PARENTONI, Leonardo. **Compartilhamento de Dados Pessoais e a figura do Controlador**. Disponível em: https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller Acesso em 04/09/2023

[117] "Segundo a ANPD, incidente de segurança é um evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais,

Outro requisito fundamental para a proteção de dados pessoais em cidade inteligente é a garantia do processamento de dados justo e imparcial. Porém, a falta de transparência sobre o tratamento de dados pessoais nesse contexto, em especial quando e como os dados pessoais são coletados e tratados, dificulta o alcance dessa garantia. Isto pode encobrir a ocorrência de discriminações algorítmicas[118] em cidades inteligentes e prejudicar pessoas vulneráveis, como já ocorreu em outras situações envolvendo tecnologias que são aplicadas no ambiente urbano[119].

Como se não bastasse, é preciso atentar para os incidentes de segurança dos dados pessoais em cidade inteligente. Ainda existem grandes limitações da própria tecnologia para a segurança dos dados pessoais coletados no ambiente urbano, como em situações de compartilhamento de dados pessoais entre dispositivos IoT e de armazenamento dos dados pessoais em nuvem (*cloud computing*).

As empresas prestadoras de serviços tecnológicos ou fornecedoras de produtos de tecnologia que utilizam dados pessoais também devem se atentar à proteção dos dados pessoais desde a concepção do seu serviço ou a criação do seu produto. A exigência técnica e jurídica sobre a proteção de dados pessoais será cada vez maior e a empresa que já investe neste quesito sairá beneficiada.

Outro problema sério em cidades inteligentes é o risco do monitoramento excessivo (*bulk surveillance*)[120], seja pelos governos ou pelas próprias empresas privadas controladoras dos dados. Por anos, empresas são demandadas pelos governos a oferecer acesso ao seu banco

---

independentemente do meio em que estão armazenados". GOV.BR. Autoridade nacional de Proteção de Dados. **Comunicação de incidente de segurança.** 23/12/2022 Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis#:~:text=%C3%89%20um%20evento%20adverso%20confirmado,meio%20em%20que%20est%C3%A3o%20armazenados. Acesso em 05/09/2023

[118]O significado de algoritmo, por Ana Frasão: "Nesse sentido, algoritmos são fórmulas ou receitas para execução de tarefas, soluções de problemas, realizações de julgamentos e tomadas de decisões. Como tal, existem há muito tempo, sendo comum a referência ao algoritmo de Euclides, o famoso matemático grego, como uma das primeiras – senão a primeira – iniciativas nesse sentido. Só mais recentemente, no século XX, é que os algoritmos passaram a ser vistos no âmbito da ciência da computação como sequências finitas de ações executáveis para a solução de um problema específico*"*. Para mais informações, vide FRASÃO, Ana, **Discriminação algorítmica. Compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade-parte 1.** 16/06/2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://professoraanafrazao.com.br/files/publicacoes/2021-06-16-Discriminacao_algoritmica_Compreendendo_o_que_sao_os_julgamentos_algoritmicos_e_o_seu_alcance_na_atualidade_Parte_I.pdf 1 p. Acesso em: 10/05/2023

[119]CERULLO, MEGAN. **How companies get inside gig workers' heads with "algorithmic wage discrimination".** CBS NEWS. 18/04/2023. Disponível em https://www.cbsnews.com/news/algorithmic-wage-discrimination-artificial-intelligence/ Acesso 10/05/2023

[120] Monitoramento em massa é uma prática governamental de coletar um amplo volume de dados sob uma finalidade específica, ao menos superficialmente. Um exemplo é a coleta de dados em massa em prol da segurança contra atentados terroristas. A coleta de dados em massa envolve, além das informações colhidas pelo setor público, a posse governamental de registros do setor privado. A preocupação de ativistas que defendem a privacidade está na falta de supervisão sobre esses programas de coleta de dados em massa e na forma indiscriminada em que essa coleta de informações pode ocorrer.

de dados, o que ocorreu, por diversas vezes, sem a observância de qualquer princípio ou dispositivo do ordenamento jurídico da proteção de dados pessoais.

Atualmente, o monitoramento excessivo é um tema debatido em todo mundo, inclusive no Brasil[121]. A ocorrência desse fenômeno é frequente na cidade inteligente e ocorre em várias escalas, mesmo em pequenos serviços urbanos que parecem ser inofensivos, a exemplo do serviço de limpeza urbana em Londres[122].Neste caso, foram instalados dispositivos em lixeiras "inteligentes" que rastreavam os telefones dos pedestres com o propósito de vender dados pessoais para comerciantes que, por sua vez, direcionavam anúncios conforme o perfil do cidadão.

Uma vez apontados os desafios encontrados para a proteção de dados pessoais em cidades inteligentes, passa-se a analisá-los, detalhadamente, no Capítulo 1. Por fim, o Capítulo 2 traz alguns caminhos criativos, adotados no estrangeiro, para enfrentar esses problemas.

1.4. Radar Tecnológico – Cidades Inteligentes (ANPD)

No final de janeiro de 2024, a ANPD lançou a nova série de publicações técnicas Radar Tecnológico, que trata sobre as tecnologias emergentes que estão impactando ou irão impactar a proteção de dados nacional e internacional. O Radar Tecnológico não tem a intenção de esgotar os temas abordados ou firmar posicionamentos institucionais [123].

O primeiro volume da série tratou, especificamente, das cidades inteligentes. Foram citados alguns dos seus principais conceitos, as suas potencialidades e perspectivas, sob o enfoque da proteção dos dados pessoais no Brasil.

---

[121] Notícias sobre monitoramento na Índia, no País de Gales, no Canadá, no Brasil e na Austrália, respectivamente. BBC NEWS. CCTV: **Why do so many Indians love surveillance?** 30 March 2023. Disponível em: https://www.bbc.com/news/world-asia-india-65115110 Acesso em 05/09/2023. BBC NEWS. **CCTV: Welsh police and government off Chinese Hikvision cameras**. 16 February 2023. Disponível em: *https://www.bbc.com/news/uk-wales-64629861* Acesso em 05/09/2023. CBC NEWS**. Sidewalk Labs proposed neighborhood remains a lightning rod for privacy concerns**. May 2018. Disponível em: https://www.cbc.ca/news/canada/toronto/sidewalk-labs-privacy-concerns-1.4644449 Acesso em 05/09/2023. VEJA SÃO PAULO. **Smart Sampa: Justiça autoriza compra de câmeras com reconhecimento facial**. Disponível em: https://vejasp.abril.com.br/cidades/smart-sampa-justica-autoriza-compra-de-cameras-com-reconhecimento-facial; Acesso em 05/09/2023. DIGITAL RIGHTS WATCH. ***Australia s new mass surveillance mandate.*** September 2021. Disponível em: https://digitalrightswatch.org.au/2021/09/02/australias-new-mass-surveillance-mandate/ Acesso em 05/09/2023.

[122] SEWARD, Zachary M; DATOO, Siraj. **City of London halts recycling bins tracking phones of passers-by.** QUARTZ. 12/08/2013. *Disponível em:* https://qz.com/114174/city-of-london-halts-recycling-bins-tracking-phones-of-passers-by Acesso em 05/05/2023

[123] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **RADAR TECNOLÓGICO. ANPD lança nova série de publicações técnicas.** 29/01/2024. Disponível em**:** https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-serie-de-publicacoes-tecnicas-com-o-tema-cidades-inteligentes

Em razão da data da sua publicação, às vésperas da defesa dessa dissertação, não foi possível analisar este material com maior profundidade. No entanto, o seu recente lançamento *reforça a importância da hipótese abordada neste estudo, bem como a sua atualidade*.

As principais preocupações listadas pela ANPD para a proteção de dados pessoais em cidades inteligentes são: a vigilância e o controle; o uso comercial dos dados; o desvio de finalidade; o vazamento dos dados; o compartilhamento indevido; a discriminação e aspectos éticos e; a perda da qualidade dos dados.

Já as medidas de mitigação de riscos à proteção de dados pessoais em cidades inteligentes citadas pela a ANPD são: a criação de programa de privacidade; a imposição de alto nível de segurança cibernética; a promoção de programas de conscientização e de participação popular; o armazenamento local dos dados; a minimização dos dados; a gestão de fornecedores; a promoção do *privacy by design*; a anonimização e pseudoanonimização de dados e; a gestão de medidas antidiscriminatórias.

Com se verá a seguir, *tanto os desafios como as medidas de mitigação citados pela ANPD são semelhantes aos abordados neste trabalho*. Além disso, este estudo irá tratar da *smart city* em Londres, implantação de tecnologia no ambiente urbano apontada pelo Radar Tecnológico da ANPD como um case de sucesso.

CAPÍTULO II: A PROTEÇÃO DE DADOS PESSOAIS EM CIDADES INTELIGENTES

Este capítulo trata das incongruências da implantação de tecnologia *smart city* no ambiente urbano para a proteção de dados pessoais, identificadas no tópico anterior. Conforme explicado na Introdução, o enfoque principal deste trabalho é a análise *jurídica* da proteção dos dados pessoais em situações que envolvem tecnologia de *smart city* e não o estudo aprofundado das inovações tecnológicas.

Desse modo, este capítulo pesquisa as limitações da tecnologia na garantia dos direitos relativos à proteção de dados pessoais bem como às liberdades civis e garantias fundamentais do cidadão. Também, identifica desafios jurídicos que dificultam a eficácia e a adequação do sistema de proteção de dados pessoais no contexto tecnológico, que podem interromper a inovação ou diminuir os benefícios que as tecnologias proporcionam para os cidadãos.

Para fins didáticos, este capítulo foi dividido em tópicos que tratam de assuntos específicos encontrados e citados no capítulo anterior. Em cada um deles são abordados tópicos sobre direito, inovação e tecnologia.

Com efeito, o objetivo é oferecer um panorama sobre o tema, criando um ponto de partida para estudos mais aprofundados sobre o assunto de cada item. Afinal, a correta identificação dos problemas jurídicos existentes neste ambiente é o primeiro passo para solucioná-los.

Para atingir esta meta, foram utilizados materiais do estrangeiro sobre as tecnologias *smart city*, o sistema de proteção de dados pessoais e casos concretos, especificamente em regiões onde a implantação dessa tecnologia está mais avançada do que no Brasil. Entende-se como fundamental aproveitar as lições extraídas do exterior, pois, futuramente, as cidades brasileiras viverão desafios semelhantes ou mesmo idênticos.

Ainda, verificam-se casos concretos sobre tecnologias disruptivas no Brasil, identificando a posição jurisprudencial e da ANPD sobre assuntos ligados à proteção de dados pessoais. Destacam-se os dispositivos legais importantes para a proteção de dados pessoais em cidade inteligente brasileiras, preparando a investigação sobre os desafios jurídicos para a proteção de dados pessoais neste ambiente.

Finalmente, abordam-se, de forma sucinta, os sistemas de proteção de dados pessoais comunitário europeu e estadunidense, por serem referências para o ordenamento de proteção de dados pessoais brasileiro e terem entendimentos distintos sobre o tema. Também são analisados alguns dispositivos do sistema de proteção de dados pessoais do Reino Unido, região

avançada na implantação de tecnologia *smart city* e que possui iniciativas próprias, diferentes daquelas existentes no modelo comunitário europeu.

2.1. Questões preliminares à Proteção de Dados Pessoais:

Este tópico explica, de maneira propositadamente sucinta, o ordenamento de proteção de dados pessoais brasileiro. Identifica o seu conjunto normativo e outros dispositivos jurídicos importantes, que estão espalhados pelos diplomas legislativos nacionais, para a implantação de tecnologia no ambiente urbano.

Para fins didáticos, aborda os instrumentos normativos brasileiros que tratam sobre a proteção de dados pessoais em ordem temporal, ou seja, *da legislação mais antiga até a mais recente*. De igual forma, analisa, em ordem cronológica, decretos que fazem parte do sistema de proteção de dados pessoais e que têm relevância para a implantação da tecnologia *smart city*.

A Lei n. 13.709, do ano de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD) é a lei brasileira que dispõe sobre o tratamento de dados pessoais[124]. No entanto, a LGPD não é o único instrumento normativo que trata sobre o assunto e, tampouco, é o primeiro.

Por conta disso, quem pretende implantar dispositivos de cidade inteligente que utilizam dados pessoais em ambiente urbano brasileiro deve observar, além da LGPD, outros diplomas legislativos, alguns deles tratados neste texto. Cada setor de serviço ou produto destinado a atender os cidadãos tem as suas particularidades jurídicas, e, portanto, o desenvolvedor de tecnologia deve se atentar à legislação específica da sua área de atuação.

A Declaração Universal de Direitos Humanos, de 1948, a qual o Brasil aderiu, prevê, em seu artigo 12, o direito à vida privada.[125] Essa regra foi adotada em vários sistemas jurídicos, a exemplo da Constituição Brasileira de 1988, a partir do artigo 1º inciso III, que dispõe sobre a cláusula geral da dignidade da pessoa humana.

---

[124] O objeto da LGPD: "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"

[125] "Artigo 12. Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques." UNITED NATIONS. **Universal Declaration of Human Rights – Portuguese**. 1948 Disponível em https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por

Da dignidade humana também se irradiam vários direitos da personalidade, como honra, imagem, identidade pessoal, proteção de dados pessoais e privacidade. Estes direitos conferem autonomia física e moral ao cidadão para conduzir a sua vida[126].

Inclusive, a Constituição brasileira de 1988 adotou, desde o seu texto inicial, a proteção constitucional dos direitos da personalidade, entre eles, os direitos à informação, à vida privada e à intimidade[127]. Em seu artigo 5º, incisos X[128] e XII[129], o diploma garante os direitos à privacidade, ao sigilo de correspondência, às comunicações telegráficas, de dados e às comunicações telefônicas como direitos e garantias fundamentais.

Aqui, ganha destaque o direito à privacidade e a sua inserção em outros diplomas legislativos ordinários de diferentes naturezas como os regramentos civil, processual, penal, comercial e tributário[130]. A pessoa que pretende desenvolver um dispositivo ou um aplicativo voltado para a cidade, também deve ficar atenta às regras de privacidade, não apenas da LGPD ou da CF/88, mas àquelas normas decorrentes da área em que a tecnologia será implantada.

Ainda na CF/88, destaca o inciso LXXII[131] do mesmo artigo 5º, que criou o remédio constitucional do *habeas data*, estabelecendo um instrumento para proteger o direito de acesso e retificação de dados pessoais[132]. A Lei 9.507/97 regulamentou o *habeas data* e materializou a garantia desses direitos, através da criação do rito processual desse remédio constitucional.

Por fim, mas não menos importante, há a emenda constitucional de nº 115/2022 que acrescentou, de forma expressa, os dados pessoais no rol dos direitos e garantias fundamentais

---

[126] MARTINS, Guilherme Magalhães. **A lei Geral de Proteção de Dados Pessoais (LEI 13.709/2018) e a sua principiologia.** Revista dos Tribunais Online. Thomson Reuters, Vol. 1027/2021. 203 -243 p. Maio de 2021. 2 p.

[127] A Constituição brasileira em seu artigo 5° incisos XXXIII e °, XXXIV, versam sobre o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos e o direito à obtenção de certidões de repartições públicas, respectivamente.

[128] Artigo 5º da Constituição Brasileira de 1988. "Inciso *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;"

[129] Artigo 5º da Constituição Brasileira de 1988. "Inciso 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;"

[130] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020. 283 p.

[131] Artigo 5º da Constituição Brasileira de 1988. "Inciso LXXII - conceder-se-á "habeas-data":a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo";

[132] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados**. Revista dos Tribunais. 2ª edição. 2020. 283 p.

do artigo 5º[133] e fixou a competência privativa da União para legislar sobre o tema[134]. Antes dessa emenda, o STF já reconhecia o direito de proteção de dados pessoais como um direito autônomo[135].

Passando para os diplomas infraconstitucionais, a Lei 8.078, de 1990, que instituiu o Código de Defesa do Consumidor, contempla, em seus artigos 43 e 44, os preceitos sobre a proteção de dados pessoais em relações jurídicas de consumo. O artigo 43[136] estabelece os direitos e as garantias do consumidor sobre as informações pessoais presentes em banco de dados e cadastros.

Portanto, todas as entidades que implantam tecnologias *smart city* e que tenham caracterizado uma relação de consumo com o cidadão devem observar os ditames do CDC. Como será verificado em item posterior, os cadastros e registros de proteção ao crédito, de naturezas pública e privada, bem como as organizações comerciais e estatais que "alimentam" esses bancos de dados, devem observar os direitos do consumidor, como a retificação de dados incorretos.

Uma lei importante para a regulação da internet e da proteção de dados pessoais é a Lei de Direitos Autorais nº 9.610/1998. Todavia, ainda é aguardada a sua reforma, necessária para modernizar a legislação quanto aos direitos do autor no mercado único digital.

Já a Lei nº 12.527 de 2011 (Lei de Acesso à Informação - LAI), traz os procedimentos a serem observados, principalmente pelas entidades públicas, para a garantia do direito de acesso à informação do cidadão. Esta lei defende, como regra geral, a publicidade das

---

[133]Artigo 5º da Constituição Brasileira de 1988. "Inciso LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais*"*.

[134]Art. 21 da Constituição Brasileira de 1988. *Compete à União: "*XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. Art. 22. Compete privativamente à União legislar sobre: XXX - proteção e tratamento de dados pessoais".

[135]BRASIL. Supremo Tribunal Federal. STF *s***uspende compartilhamento de dados de usuários de telefonias com IBGE.** 07/05/2020. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1

[136]"Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (Vigência)" Lei 8.078/1990. **Código de Defesa do Consumidor.**

informações, a divulgação de informações de interesse público mesmo sem solicitação e a transparência na administração pública[137].

Em 2014, foi criada a Lei 12.965, intitulada de Marco Civil da Internet (MCI), diploma que estabelece os padrões para a aplicação dos direitos fundamentais na internet[138]. Dentre os seus princípios, constam, além da reprodução da CF/88, em seu artigo 7º inciso I, sobre os direitos de inviolabilidade da intimidade, da vida privada, da honra e da imagem no ambiente digital, há os direitos da privacidade e da proteção dos dados pessoais[139].

Na época em que o MCI foi elaborado, havia urgência na criação de dispositivos que regulassem o tratamento de dados pessoais, principalmente pela repercussão do caso Snowden[140]. Apesar da existência de um projeto de lei semelhante à LGPD, optou-se por transferir algumas regras de tratamento de dados pessoais desse projeto para o MCI, já que a sua tramitação legislativa estava mais avançada[141].

---

[137]. "Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - observância da publicidade como preceito geral e do sigilo como exceção; II - divulgação de informações de interesse público, independentemente de solicitações; IV - fomento ao desenvolvimento da cultura de transparência na administração pública." Lei de nº12.527/2011**. Lei de Acesso à Informação.**

[138] "Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria." Lei nº 12.965/2014**. Marco Civil da Internet.**

[139] "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;" **Lei nº 12.965/2014. Marco Civil da Internet.**

[140]THE GUARDIAN. **Snowden NSA files surveillance revelations decoded.** 2013. Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

[141]SOUZA, Carlos Afonso; LEMOS, Ronaldo. **Marco Civil da Internet. Construção e aplicação**. Editar Editora associada. 2016. Juiz de Fora- MG 28 p.

Alguns exemplos sobre à proteção de dados pessoais no MCI são os artigos 7 º[142], 10[143], 11[144] e 16 º[145]. Além desses artigos, houve dispositivos originários que enfrentaram críticas e foram retirados do MCI, como a possibilidade de se obrigar empresas estrangeiras que coletam dados pessoais no Brasil a manter servidores no território nacional[146].

Apesar de conter regras de tratamento de dados pessoais no ambiente online, o MCI é considerado uma lei geral em comparação à LGPD. Isto é verdade pois o MCI trata, além da proteção dos dados pessoais, de vários assuntos ligados à internet, e a LGPD aborda, de forma específica, a proteção dos dados pessoais[147].

A inserção de normas relativas à proteção dos dados pessoais no MCI gerou uma série de problemas entre os seus dispositivos e algumas regras da LGPD, que, se não forem dadas as devidas interpretações, podem apresentar contradição. Os maiores exemplos desses possíveis conflitos entre as duas leis são quanto à forma de consentimento do titular para o tratamento de

---

[142]" Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (Redação dada pela Lei nº 13.709, de 2018) (Vigência")" Lei nº 12.965/2014**. Marco Civil da Internet.**

[143]"Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º "Lei nº 12.965/2014. **Marco Civil da Internet.**

[144] Art. 11. "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros." Lei nº 12.965/2014**. Marco Civil da Internet.**

[145]"Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais. (Redação dada pela Lei nº 13.709, de 2018) (Vigência)" Lei nº 12.965/2014. **Marco Civil da Internet.**

[146] SOUZA, Carlos Afonso; LEMOS, Ronaldo. **Marco Civil da Internet. Construção e aplicação**. Editar Editora associada. 2016. Juiz de Fora- MG 29 p.

[147] PARENTONI, Leonardo. LIMA, Henrique Cunha Souza. *Proteção de dados pessoais no Brasil: Antinomias Internas e Aspectos Internacionais*. Disponível em: https://www.researchgate.net/publication/340005766_Protecao_de_Dados_Pessoais_no_Brasil_Antinomias_Internas_e_Aspectos_Internacionais 25-26 p. Acesso em 12/05/2023 https://www.researchgate.net/publication/340005766_Protecao_de_Dados_Pessoais_no_Brasil_Antinomias_Internas_e_Aspectos_Internacionais Acesso em 12/05/2023 24 p. e seguintes

dados pessoais e às sanções administrativas aplicáveis a controladores e operadores em caso de descumprimento legal[148].

O Decreto de nº 9.637/2018[149] intitulado de Plano Nacional de Segurança da informação, trata da governança da segurança da informação e deve ser observado na implantação de tecnologia *smart city.* Em seu artigo 2º, o decreto propõe que a segurança da informação deve conter a *defesa cibernética, a segurança física e a proteção de dados organizacionais e, as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de informação*[150].

Estabelece, em seu artigo 3º inciso II, a proteção de dados pessoais, a proteção à privacidade e o acesso à informação como princípios do PNSI. Em seu artigo 6º inciso V, objetiva ações estratégicas relacionadas à proteção contra o vazamento de dados. O referido decreto também cria um Comitê Gestor de Segurança da Informação, nomeando como um dos seus integrantes a ANPD[151].

Outro decreto muito importante para a tecnologia *smart city* é o de nº 9.854, de junho de 2019, que institui o Plano Nacional de Internet das Coisas (PNIC) e dispõe sobre sistemas de comunicação entre máquinas e dispositivos IoT. Este decreto revogou o decreto de nº 8.234, de 2 de maio de 2014, que estabelecia um conceito sobre a comunicação entre máquinas e atribuía a ANATEL (Agência Nacional de Telecomunicações), a função de fiscalizar e regulamentar estes sistemas, mas sob as normas do Ministério das Comunicações[152].

Agora, o PNIC vincula a fiscalização e a regulamentação da ANATEL às normas do Ministério de Estado da Ciência, Tecnologia, Inovações e Comunicações (MECTIC). Ainda, o novo decreto confere ao Ministro de Estado do MECTIC, entre outras prerrogativas, a indicação de cidades para a aplicação prioritária de soluções em IoT.

---

[148]PARENTONI, Leonardo. LIMA, Henrique Cunha Souza**. Proteção de dados pessoais no Brasil: Antinomias Internas e Aspectos Internacionais.** Disponível em: https://www.researchgate.net/publication/340005766_Protecao_de_Dados_Pessoais_no_Brasil_Antinomias_Internas_e_Aspectos_Internacionais Acesso em 12/05/2023 24 p. e seguintes.

[149] BRASIL, Decreto nº 9.637, de 25 de junho de 2018. **Plano Nacional de Segurança da Informação.** 26 de dezembro de 2018. Diário Oficial da União. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm

[150] BRASIL, Decreto nº 9.637, de 25 de junho de 2018. **Plano Nacional de Segurança da Informação.** 26 de dezembro de 2018. Diário Oficial da União. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm Artigo 2º

[151] BRASIL, Decreto nº 9.637, de 25 de junho de 2018**. Plano Nacional de Segurança da Informação.** 26 de dezembro de 2018. Diário Oficial da União. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm Artigo 9º,

[152] BRASIL, Decreto nº 9.854, de 25 de junho de 2019. **Plano Nacional de Internet das Coisas.** 26 de junho de 2019. Diário Oficial da União. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm

O PNIC também criou a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas - Câmara IoT - que irá promover e criar parcerias, entre entes públicos e privados, para alavancar os interesses do PNIC. Entre outras atribuições, a Câmara IoT também irá monitorar e avaliar as iniciativas de implementação dessa tecnologia.

Por fim, o referido decreto menciona, em seu artigo 1º, a observância da proteção dos dados pessoais na implantação do Plano Nacional de Internet das Coisas. No entanto, não há nenhuma regra específica sobre o tema para este ambiente.

Apesar dos diversos instrumentos legislativos supracitados, não há, até o momento da confecção deste estudo, qualquer dispositivo legislativo *específico* sobre a proteção de dados pessoais no contexto de uma cidade inteligente. Mesmo com a tramitação do Projeto de Lei nº 976/21, intitulado de Política Nacional de Cidades Inteligentes (PNCI), não há previsão sobre a criação de uma norma específica para o tema.

Assim como os decretos sobre a segurança da informação e sobre a IoT, a PNCI traz princípios e diretrizes relativos à privacidade e à segurança dos dados, o compartilhamento dos dados, a transparência e a publicidade dos dados e das informações, em seu artigo 4º, inciso V[153] e artigo 5º, incisos IV, VI e XIV[154]. Contudo, o projeto tem a intenção de transferir a responsabilidade de regulamentar a proteção de dados pessoais nas cidades inteligentes para a LGPD [155], sendo este um desejo expresso do legislador[156].

---

[153] "Art. 4º A cidade inteligente deverá ser regida pelos seguintes princípios: V – privacidade dos cidadãos e segurança dos dados;" BRASIL. CAMARA DOS DEPUTADOS. Projeto de lei 976.2021**. Política Nacional de Cidades Inteligentes (PNCI),** Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449

[154] "Art. 5º O desenvolvimento de iniciativas de cidades inteligentes deverá observar as seguintes diretrizes: IV – integração de bancos de dados do Poder Público mediante o uso de padrões de interoperabilidade; VI – compartilhamento de dados e informações entre entes federativos; XIV – transparência e publicidade de dados e informações, sem prejuízo à privacidade da população e à segurança dos dados;" BRASIL. CAMARA DOS DEPUTADOS. Projeto de lei 976.2021. **Política Nacional de Cidades Inteligentes (PNCI)** Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449

[155] "Art. 5º O desenvolvimento de iniciativas de cidades inteligentes deverá observar as seguintes diretrizes: XIV – transparência e publicidade de dados e informações, sem prejuízo à privacidade da população e à segurança dos dados; § 2º A observância da privacidade e da segurança de que trata o inciso XIV deverá levar em consideração a necessária garantia da proteção dos dados pessoais e o uso das melhores práticas, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018". BRASIL. CAMARA DOS DEPUTADOS. Projeto de lei 976.2021**. Política Nacional de Cidades Inteligentes (PNCI),** Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449

[156] "Com relação aos aspectos do uso de dados, em primeiro lugar, é importante ressaltar que esse tipo de iniciativa deve se inserir em um contexto maior e específico ditado pela LGPD – Lei Geral de Proteção de Dados, instituída pela Lei no 13.709, de 2018. Assim, o uso de dados pela Administração em projetos de cidades inteligentes deve observar as restrições e o ordenamento contido na LGPD, em especial a observância da privacidade e da segurança das informações, assim como o uso das melhores práticas. A integração dos serviços e o compartilhamento de dados entre entes da Administração deverão seguir estritamente as regras lá contidas que estabelecem, entre outros ditames, que o tratamento deve se dar para a execução de políticas públicas específicas e aprovadas. Da mesma forma, os dados coletados não podem objetivar sua comercialização de forma identificada. Todos esses cuidados devem continuar a serem seguidos." BRASIL. CAMARA DOS DEPUTADOS. Projeto de lei 976.2021**. Política**

Portanto, mesmo com a aprovação do projeto de lei de nº 976/21, a entidade que pretenda implantar a tecnologia *smart city* terá que observar todo o ordenamento jurídico sobre proteção de dados pessoais descrito anteriormente, além de legislações específicas do seu setor de atuação.

2.2. Volume, qualidade e estruturação dos dados

Este item detalha os problemas da utilização das tecnologias de armazenamento, processamento e transferência de dados, como nos casos de uso do *big data* e do *cloud computing,* em cidades inteligentes. Especificamente, estudam os riscos à proteção de dados pessoais causados pelo tratamento de grande volume de dados de má qualidade e sem formato previamente estruturado.

Cidades inteligentes estão gerando, em tempo real, conjuntos de dados enormes, variados e interconectados para a prestação de um serviço público "inteligente". Este dilúvio de dados coletados e analisados busca fornecer maiores compreensão e controle do ambiente urbano.

O *hype* da cidade inteligente está diretamente relacionado com a esperança no *big data* para a transformação do conhecimento e da governança das cidades. Esta tecnologia de baixo custo operacional e flexível tornou possível o acesso das regiões de menor poder de investimento à tecnologia de cidade inteligente e o desenvolvimento de diversos aplicativos em vários setores dos serviços urbanos[157].

Por conta da importância do *big data* na tecnologia *smart city* e pelas suas características serem relevantes para a discussão sobre a proteção de dados pessoais em cidades inteligentes, importa aprofundar sobre a sua natureza. Frisa-se que este estudo não tem a intenção de esgotar o tema, mas de entender a tecnologia para o fim de identificar os desafios à proteção de dados pessoais na sua utilização em cidades inteligentes.

Nacional de Cidades Inteligentes (PNCI), Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449 19 p.

[157]"In other words, big data consists of massive, dynamic, varied, detailed, inter-related, low cost data sets that can be connected and utilized in diverse ways, thus offering the possibility of studies shifting from: data-scarce to data-rich; static snapshots to dynamic unfolding's; coarse aggregation to high resolution ; relatively simple hypotheses and models to more complex, sophisticated simulations and theories" KITCHIN, Rob, **The Real-Time City? Big Data and Smart Urbanism** GeoJournal 79(1):1-14, 2014, Available at SSRN: https://ssrn.com/abstract=2289141 or http://dx.doi.org/10.2139/ssrn.2289141

Não há um consenso sobre o conceito de *big data*[158]. Um dos motivos dessa indefinição é o constante desenvolvimento tecnológico, pois o que era considerado *big data* no passado, não é mais nos dias atuais e, certamente, não o será em um futuro próximo[159].

Em se tratando de um conceito simples e geral, o termo *big data* se refere a um banco de dados que coleta, gera, altera, armazena e analisa quantidades massivas de dados rapidamente. É uma tecnologia capaz de coletar uma grande variedade de tipos de dados, sejam eles estruturados em números ou categorias ou dados não estruturados, como e-mails e textos[160].

O *Information Comissioner s Office* (ICO), agência governamental do Reino Unido[161] adere ao conceito de *big data* descrito no *IT Gartner Glossary* [162], o qual enfatiza três características da tecnologia, sendo elas o volume, a variedade e a velocidade (3Vs). Estas características também são comumente citadas por parte da doutrina[163].

Todavia, o conceito de *big data* evoluiu e, por conta disso, tratá-lo apenas citando os 3Vs se tornou uma definição incompleta[164]. Além de vago, este conceito não estabelece uma linha divisória clara entre um banco de dados comum e o *big data*[165].

O termo *big data* deve ser mais amplo e se refere a dados em grande escala, que não podem ser feitos em escalas menores, e servem para extrair insights ou criar valor, de tal modo que revolucionam os mercados, as organizações e a relação entre pessoas e entre cidadãos e

---

[158]MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle. 15.p

[159] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.** 2014. 13 p.

[160]FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.** 2014. 26 p.

[161] INFORMATION COMISSIONER S OFFICE (ICO). **Big data, Artificial Intelligence, Machine Learning and Data Protection.** Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf 6 p. e seguintes

[162] ***Big data*** *is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation*. INFORMATION TECHNOLOGY GARTNER GLOSSARY. Disponível em https://www.gartner.com/en/information-technology/glossary/big-data

[163] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.** 2014**.** 13 p.

[164] Há quem critique essa definição. "One way to think about big data — There is a loud and unproductive debate over the origin of the term "big data" and how to perfectly define it. The two words have occasionally appeared in unison for decades. A research report in 2001 by Doug Laney of Gartner set out the "three Vs" of big data (volume, velocity, and variety), which was useful for its time but imperfect" MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle. 245 p.

[165] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. 2014. 14 p.

governos[166]. Deste modo, além de coletar e analisar uma imensa quantidade de dados, o *big data* pode correlacioná-los[167].

Entende-se que deve ser acrescentado a este conceito a variedade de tipos dos dados tratados no *big data*, como dados textuais, a exemplo de e-mails, páginas da web e twists; dados gerados por máquina, como dados de GPS, telefones e sensores e; dados de rede como aqueles associados a família e amigos[168].

Por conta das suas características, estudadas adiante, é inerente ao *big data* coletar e processar dados que não são úteis para a finalidade pela qual ele foi projetado. Porém, é importante lembrar que nem todos os dados coletados e tratados pelo *big data* em cidades inteligentes são pessoais, a exemplo dos dados climáticos e meteorológicos que auxiliam pesquisas desse sentido.

Com efeito, a este trabalho só interessa analisar o *big data* para a coleta e o processamento de dados pessoais, como aqueles que utilizam fontes de mídias sociais, cartões de compras, sensores de imagem e áudio para promover serviços públicos urbanos e dispositivos de monitoramento, seja para fins de segurança ou para cuidar de pessoas com problemas de saúde.

Uma vez entendida a natureza do *big data*, passa-se a analisar as suas características que impactam na proteção dos dados pessoais em cidades inteligentes. Apenas para fim didático, a análise tem início sobre o *volume* massivo de dados que o *big data* contempla.

Antes de mais nada, não existe um número fixo quantitativo de dados para classificar o *big data,* pois leva em consideração o porte da entidade que está em posse da tecnologia. O que representa um *big data* para uma empresa de pequeno porte, que possui dados de centenas de clientes, pode não significar para uma multinacional[169], por exemplo.

Todavia, o *big data* que possui um maior volume de dados tende a ser impreciso e, portanto, menos confiável. Ter uma margem de imprecisão nas informações faz parte do *big*

---

[166] MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle. 16.p.

[167]"As noted in Chapter One, big data is about three major shifts of mindset that are interlinked and hence reinforce one another. The first is the ability to analyze vast amounts of data about a topic rather than be forced to settle for smaller sets. The second is a willingness to embrace data's real-world messiness rather than privilege exactitude. The third is a growing respect for correlations rather than a continuing quest for elusive causality." MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle. 28 p.

[168]FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. *2014.* 15 p.

[169] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. *2014.* 14 p.

data e é necessário aprender a lidar com ela[170]. Inclusive, em alguns casos, as informações trazidas pelo grande volume de dados, embora menos precisas, podem agregar maior valor, o que permite renunciar ao rigor de uma exatidão estrita[171].

No entanto, quando os dados do *big data* são pessoais, tanto o tratamento excessivo, como a inexatidão dos dados representam inconsistências em relação às legislações de proteção de dados pessoais[172]. Estas violações causam prejuízos financeiros, inclusive para os desenvolvedores da própria tecnologia *smart city* [173].

Especificamente quanto à implantação do *big data* em cidade inteligente, a quantidade de dados coletados foi classificada como um dos *desafios técnicos*[174] para o desenvolvimento de políticas públicas eficientes e inovadoras nas cidades. Existe uma preocupação em identificar as informações que são consistentes e as utilizar de acordo com a necessidade de cada setor[175].

Outro problema do gigantesco volume de dados é a dificuldade do seu armazenamento. Existem cidades que não possuem tecnologia de armazenamento e optam por contratar empresas estrangeiras para armazenar os dados coletados da cidade.

Para tornar este problema ainda mais complexo, há casos em que as empresas estrangeiras contratadas compartilham dados pessoais com o seu governo ou os transferem para filiais localizadas em outros países. Dois exemplos são os casos do META (anteriormente chamada de Facebook Inc) e do aplicativo TikTok, ambos a serem estudados no tópico de compartilhamento indevido e desvio de finalidade.

---

[170] MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle. 41 p.

[171] MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle. 42 p.

[172] Como exemplos, cita as violações aos princípios da necessidade e da qualidade dos dados, constantes no artigo 6º, incisos III e V, respectivamente, da LGPD e aos princípios da minimização dos dados e da exatidão, previstos no artigo 5º do GDPR.

[173] GLOBO. PORTAL DE NOTÍCIAS DA GLOBO. **Google é multado nos EUA por coleta de dados pessoas para Street View**. 12/03/2013. Disponível em: https://g1.globo.com/tecnologia/noticia/2013/03/google-e-multado-nos-eua-por-coleta-de-dados-pessoais-para-street-view-2.html

[174] No contexto de cidade inteligente, riscos técnicos são potenciais desafios e vulnerabilidades associados à implementação e ao uso da tecnologia. Em especial, destacam-se três riscos: 1) Falha na cobertura de rede, que é o comprometimento da disponibilidade e da confiabilidade por meio na má qualidade de conectividade de rede dentro da cidade.2) Escolha da tecnologia. Ocorre em caso erro na escolha da tecnologia implantada na cidade, o que pode gerar problemas de ineficiência e compatibilidade. 3) Descontinuação da tecnologia: Risco da tecnologia implantada se tornar obsoleta e interromper as operações da cidade inteligente. Isto pode levar a substituições ou atualizações tecnológicas caras. SHARIF, Al Sharif; POKHAREL, Shaligram. Engineering Advance. **Smart City Dimensions and Associated Risks**. Sustainable Cities and Society (SCS) international journal. ScienceDirect Disponível em: https://www.sciencedirect.com/journal/sustainable-cities-and-society 7 p.

[175] D AMICO, Gaspare; L ABBATE, Pasqua; LIAO, Wenjie; **Understading Sensor Cities: Insights From Technology Giant Company Driven Smart Urbanism Practices.** MDPI. 06/08/2020. Disponível em: https://www.mdpi.com/1424-8220/20/16/4391. 13 p.

O crescimento da capacidade de utilização do *big data* potencializa este problema, pois a tecnologia está cada vez mais inserida na vida do cidadão, por meio da coleta massiva de dados derivados de cartões de crédito e débito, celulares, sensores espalhados por toda a cidade e até dentro das casas[176]. A disponibilidade dessa quantidade de dados se dá também pela sua armazenagem baseada em serviços *cloud*, tecnologia que, atualmente, vem sofrendo incidentes de segurança[177].

Além do mais, a quantidade de dados coletados pelo b*ig data* em cidade inteligente pode representar a coleta excessiva de dados pessoais, o que implica inconsistências jurídicas relativas ao sistema de proteção de dados pessoais brasileiro. O princípio da necessidade, constante no artigo 6º inciso III da LGPD, é um exemplo, pois restringe a coleta dos dados pessoais àquilo que é estritamente necessário ao cumprimento da finalidade informada ao titular dos dados[178].

Como se não bastasse, a implantação do *big data* em cidade inteligente pode representar um risco ao princípio da finalidade, este intimamente ligado ao princípio da necessidade, em casos onde o titular dos dados pessoais sequer é informado sobre o tratamento dos seus dados. O desrespeito ao dever de informação é mais grave na hipótese de o controlador dos dados necessitar do consentimento do seu titular para realizar o tratamento[179].

O princípio da finalidade é essencial para limitar o acesso de terceiros ao banco de dados, além de servir como alicerce para determinar se o uso de um dado pessoal é adequado para uma finalidade determinada. Por último, mas não menos importante, o princípio da finalidade impõe ao responsável que determine, de forma expressa, a finalidade do tratamento

---

[176]INTERNATIONAL COMMISSIONER'S OFFICE. **Big Data and Data Protection**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220 14 p. Acesso em 29/04/2023

[177] Vide alguns exemplos: **Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket: 'Lives at Stake.** Disponível em: https://www.darkreading.com/application-security/cloud-misconfig-exposes-3tb-sensitive-airport-data-amazon-s3-bucket ; **Did Anonymous Carry Out a Cyber Attack on Nestlé? Company Claims Data Leak Was Internal** Disponível em: https://www.cpomagazine.com/cyber-security/did-anonymous-carry-out-a-cyber-attack-on-nestle-company-claims-data-leak-was-internal/ *"Japanese medical online consultation site leaking consumer-submitted images of symptom".* Disponível em: https://www.databreaches.net/japanese-medical-online-consultation-site-leaking-consumer-submitted-images-of-symptoms/

[178] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Thomson Reuters Brasil Conteúdo e Tecnologia LTDA. São Paulo. 2019. 71 p.

[179] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Thomson Reuters Brasil Conteúdo e Tecnologia LTDA. São Paulo. 2019. 71 p.

dos dados, sob pena de ilegitimidade do tratamento em caso de finalidades amplas e genéricas, das quais não há limitação[180].

Aqui, ressalta a importância do princípio da finalidade para a proteção dos dados pessoais na implantação de *smart city*. A tabela *Smart City,* constante do item 1.3 deste estudo, mostra a relevância deste princípio, não apenas para o *big data,* mas para qualquer tecnologia *smart city* que utiliza dados pessoais neste ambiente.

Por exemplo, um controlador que tem autorização para tratar dados pessoais por meio do *Waggle*[181], com a finalidade de pesquisa, não pode utilizar esses dados para outros propósitos, como, para criar um perfil do cidadão ou vender informações a uma empresa de seguro. Desse modo, a finalidade bem delineada preza pelo controle sobre o uso dos dados pessoais.

A garantia de um nível de qualidade dos dados coletados pelo *big data* também é considerada um *desafio técnico* para as cidades inteligentes[182]. A qualidade dos dados interfere no desempenho das técnicas de análise de *big data*[183], e, por consequência, nos *insights* extraídos.

Este desafio se torna mais complexo quando envolve a coleta de dados sensíveis[184], como na área da saúde. Com efeito, o próprio *European Institute for Innovation through Health Data* reconhece a importância da qualidade dos dados para a tomada de decisão e inferências clínicas válidas e confiáveis[185].

A produção qualitativa de dados de saúde está diretamente ligada ao sucesso do software utilizado bem como ao nível de conhecimento dos usuários finais do sistema do *European*

---

[180] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. Thomson Reuters Brasil Conteúdo e Tecnologia LTDA. São Paulo. 2019. P 90

[181] É uma Plataforma que utiliza sensores sem fio e computação em nuvem para coletar, armazenar e analisar dados produzidos em uma cidade inteligente. WAGGLE AI. *Scientific AI at the edge.* Disponível em: https://wa8.gl/

[182] D AMICO, Gaspare; L ABBATE, Pasqua; LIAO, Wenjie; **Understanding Sensor Cities: Insights From Technology Giant Company Driven Smart Urbanism Practices.** Disponível em: https://www.mdpi.com/1424-8220/20/16/4391. 13 p.

[183]As técnicas de análise de big data são métodos utilizados para extrair insights, padrões e informações de grupos de dados grandes e complexos. Através destes métodos é possível gerir, processar e analisar o seu imenso e complexo banco de dados, criando novos padrões de análise e auxiliando a tomada de decisões. Para mais informações, CHERTOV, Oleg. MYLOVANOV Tymofiy; KONDRATENKO, Yuriy e outros. **Recent Developments in Data Science and Intelligent Analysis of Information**. Editora Springer. June 4-7,2018

[184] Em seu artigo 5º, inciso II, A LGPD considera dados sensíveis: "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 a uma pessoa natural."

[185] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality. What about EHR Data Quality?** Disponível em. https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality

Institute for Innovation through Health Data. Neste caso, os insights são utilizados para a prestação de cuidados diários de pacientes e para a investigação clínica de doenças[186].

A qualidade das informações também depende de outros componentes tecnológicos responsáveis pela coleta e pela transferência dos dados. Por conta da capacidade do *big data* de utilizar diversas fontes[187], seu banco de dados pode ser alimentado tanto por informações de sistemas internos da organização como por dados de sistemas externos de GPS, redes sociais, sensores de IoT espalhados pela cidade**,** relatórios de crédito, informações de censo, etc..[188]

Desse modo, no caso de cidade inteligente que utiliza sensores de IoT, a qualidade dos dados pode ser comprometida por transmissões incorretas de dados urbanos. Neste caso, os dados se tornam inconsistentes, não confiáveis e parciais [189].

A variedade de fontes que alimentam o *big data* também constitui um risco à proteção de dados pessoais, uma vez que quanto mais fontes são utilizadas, maior é a probabilidade de haver dados pessoais desprotegidos, violados, falsos ou desatualizados. Além disso, a quantidade de fontes dificulta o controle e a segurança dos dados pessoais em cidades inteligentes [190], questão tratada em tópico posterior.

Outra limitação identificada é sobre a interoperabilidade dos dados na utilização de diferentes sistemas de coleta, processamento e armazenamento. No caso de cidadãos que desejam mudar de serviço, é difícil descobrir onde os dados estão armazenados.[191] Isto pode impedir a aplicação prática do direito a portabilidade dos dados do titular, constante da LGPD[192] e do GDPR[193].

---

[186] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality. Quality and Trustworthiness of Systems?** Disponível em. https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality Acesso em 05/11/2023

[187]FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. *2014.* 13 p.

[188]FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. *2014.* 27 p.

[189] D AMICO, Gaspare; L ABBATE, Pasqua; LIAO, Wenjie; **Understading Sensor Cities: Insights From Technology Giant Company Driven Smart Urbanism Practices.** Disponível em: https://www.mdpi.com/1424-8220/20/16/4391. Acesso em 02/11/2023. 13 p.

[190] D AMICO, Gaspare; L ABBATE, Pasqua; LIAO, Wenjie; **Understading Sensor Cities: Insights From Technology Giant Company Driven Smart Urbanism Practices.** Disponível em: https://www.mdpi.com/1424-8220/20/16/4391. Acesso em 02/11/2023. 14 p.

[191] HOEREN, Thomas, RAISER-KOLANY, Barbara. **Big Data in Context Legal, Social and Technological Insights.** Editora Springer Open. 2018. 88 p.

[192]"Artigo 17, inciso V: portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;" Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

[193] Caput do Artigo 20, 1 do GDPR. "O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:"

Destaca-se também um desafio de ordem social, no que diz respeito à qualidade de dados, que ocorre quando o responsável pela captação e alimentação do *big data* é o ser humano. Com efeito, nas situações em que a equipe responsável pela coleta não tem nenhuma formação em gestão de dados, a qualidade dos dados é variável e, por isso, não são adequados para qualquer finalidade de reutilização[194].

Este problema ocorre no sistema do *European Institute for Innovation through Health Data,* uma vez que a maioria dos profissionais de saúde não são capacitados para gerenciar dados. Como resultado, vários estudos derivados dos dados coletados possuem uma qualidade duvidosa[195].

Quanto a possíveis desafios jurídicos, a qualidade dos dados é um princípio norteador do sistema de proteção de dados pessoais brasileiro, constante do rol do artigo 6º da LGPD, e impõe ao responsável que os dados sejam objetivos, exatos e atualizados[196]. Todavia, para garantir a qualidade, é necessário observar outros princípios legais que são a transparência do tratamento e o livre acesso.

Observados determinados limites, como, os sigilos industrial e comercial, o princípio da transparência impõe que deve ser de conhecimento público a existência de um *big data* que coleta e processa dados pessoais[197]. Este princípio não está adstrito apenas à fase de coleta dos dados, mas a todo o processo de tratamento[198].

Já o princípio do livre acesso diz respeito ao poder do titular de dados de acessar as suas informações armazenadas no *big data* e as controlar, de modo que ele possa corrigir informações incorretas, acrescentar dados pessoais ou suprimir dados obsoletos[199]. Por fim,

---

[194] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality. What about EHR Data Quality?** Disponível em. https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality Acesso em 06/11/2023

[195] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality.** Disponível em: https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality

[196] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Thomson Reuters Brasil Conteúdo e Tecnologia LTDA. São Paulo. Ano de 2019. 72 p.

[197]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020. 181 p.

[198]TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Thomson Reuters Brasil Conteúdo e Tecnologia LTDA. São Paulo. Ano de 2019. 72 p.

[199]DONEDA, Danilo***. Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados***. Revista dos Tribunais. 2ª edição. 2020. 181 p.

esse princípio também confere ao titular o direito de pedir revisão de decisões automatizadas sobre os seus dados[200].

Além disso, a má qualidade dos dados coletados e analisados por dispositivos em cidades inteligentes desrespeita outros dispositivos do sistema de proteção de dados pessoais. Uma vez que são coletados dados não precisos e, por isso, não confiáveis, há grande risco do resultado da análise do *big data* ser equivocado, ilícito e discriminatório, o que vai em desencontro com os princípios da não discriminação[201] e do *accountability*[202], que são estudados em itens posteriores.

Outra característica inerente ao *big data,* e importante para a discussão sobre a proteção dos dados pessoais em cidades inteligentes, é a formação do seu banco de dados. Sua composição se dá por diferentes tipos de dados, que podem ser estruturados ou não estruturados.

Os dados estruturados são organizados e bem definidos, no geral representados em categorias como idade, estado civil, gênero e renda de um cidadão. Já os dados não estruturados são difíceis de categorizar, por não terem uma definição clara, como é o caso de textos, imagens e áudios [203].

A título de exemplo, para verificar a validade de um banco de dados que contém datas de nascimento, basta conferir se o dia, o mês e o ano estão dentro dos limites permitidos, excluindo aquelas datas que estão no futuro ou há centenas de anos no passado. Porém, verificar a validade de uma foto ou um áudio requer um processo de estruturação [204].

O trabalho de formatar o dado é a principal diferença entre dados estruturados e dados não estruturados[205]. Para ser analisado, a estruturação do dado deve estar em formato numérico ou categórico[206].

---

[200] "Art. 9: O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso*"* Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

[201]"Art. 6º inciso IX: não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos." Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

[202] "Art. 6º inciso 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." Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

[203]FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. 2014. 13 p.

[204] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. 2014. 109 p.

[205] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.**. 2014. 86 p

[206] Como o próprio nome diz, os dados numéricos são representados pelo valor quantitativo, permitindo operações matemáticas e análises quantitativas. Já os dados categóricos são qualitativos e podem ser classificados ou agrupados com base em categorias ou rótulos distintos, como, gênero, cor e tipo de produto. Para mais informações: SAID, Alan; TORRA, Vicenç. **Data Science in Practice.** Studies in Big Data. 46. Ed. Springer. 2018.

A estruturação de dados requer grande poder de processamento e, por isso, maior investimento. Há também um risco em dispender recursos financeiros com a formatação de dados não estruturados que não acrescentariam informações de valor.[207]

Conforme se extrai da tabela *Smart City*, descrita no item 1.3 deste estudo, é comum a coleta de dados não estruturados, diga-se, fotos, vídeos, áudios, entre outros, para diversas finalidades. Como exemplos marcantes, citam-se os projetos de segurança *Switching* on Darwin na Australia, que usa sistema de CCTV para captação de áudio e imagem, e o *Smart Sampa* em São Paulo, que utiliza câmeras com reconhecimento facial.

Os dados não estruturados possuem um grande valor em diversos setores da economia e planejamento urbano, inclusive para a implantação de tecnologia *smart city*. Por conta disso, muitas empresas e organizações estão investindo em tecnologias adaptadas para dados não estruturados em grande escala e em tempo real. [208]

No entanto, os dados não estruturados ainda representam desafios para a sua utilização como o aprimoramento de técnicas especializadas para extrair insights. Além do mais, não há garantia da precisão ou da qualidade dos dados não estruturados obtidos de fontes externas do *big data*, pois outras pessoas são responsáveis por essas fontes[209].

Através do estudo sobre a inserção de tecnologias de armazenamento, coleta, processamento e análise de dados em ambiente de cidade inteligente, foi possível identificar obstáculos técnicos para a promoção da proteção de dados pessoais. Estas barreiras tecnológicas, especialmente quanto ao *big data,* refletem incongruências com dispositivos basilares das legislações específicas de proteção de dados pessoais.

Os desafios jurídicos destas tecnologias estão em garantir a observância aos princípios da necessidade, da qualidade dos dados, da finalidade, da transparência no tratamento de dados e do livre acesso. Por fim, destaca-se o desafio de exercer o direito a portabilidade dos dados do titular, pela dificuldade de encontrar o local onde os seus dados estão armazenados.

2.3. Privacidade

Este item estuda, de forma intencionalmente sucinta, o conceito de privacidade e a diferença desse direito para a proteção de dados pessoais. Após, busca identificar desafios,

---

[207] FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.** 2014. 66 p.
[208] SAID, Alan; TORRA, Vicenç. **Data Science in Practice.** Studies in Big Data. 46. Ed. Springer. 2018. 117 p.
[209]FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.** 2014. 180 p.

técnicos e jurídicos, sobre a privacidade dos cidadãos no contexto de implantação de *smart city*, por meio de pesquisas específicas, e destacar a importância de estudos nacionais sobre o assunto.

Apesar de ser um direito distinto da proteção de dados pessoais, entende-se importante abordar a privacidade em cidade inteligente pelos seguintes motivos: Há vários estudos internacionais, de ordem técnica ou jurídica, sobre o tema; Há poucos trabalhos sobre privacidade em tecnologia *smart city* no Brasil; e; o tema é relevante e atual, especialmente porque a tecnologia *smart city* começou a ser implantada no Brasil.

Por possuir uma vasta história repleta de debates, o direito à privacidade[210] é um tema complexo, controverso, amplo e com vários significados. Com efeito, este estudo sobre a privacidade tem caráter meramente introdutório, por não ser o objeto desse trabalho, e tem a finalidade única de preparar a análise da privacidade no contexto de cidade inteligente.

A origem jurídica moderna do conceito de privacidade nasceu do famoso artigo americano intitulado *the right to privacy*[211], publicado em 1890 pela revista de Direito da Universidade de Harvard, por *Samuel Warren* e *Louis Brandeis.* Nesta obra, os autores definiram a privacidade como "*right to be let alone"*, que em português significa o direito de ser deixado só[212].

O contexto social, econômico e acadêmico do final do século XIX, descrito por *Warren* e *Brandeis*, remete a uma inevitável comparação com a implantação das tecnologias *smart city* nas cidades. No século XIX já havia a preocupação jurídica com a violação à privacidade, na época capitaneada pela indústria da comunicação, que usava de tecnologias disruptivas para publicar, em larga escala e com imagens, periódicos sobre a vida privada das pessoas. [213]

---

[210]Para aprofundar o estudo sobre a evolução do direito à privacidade, este autor sugere o livro de Danilo Doneda. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados**. Revista dos Tribunais. 2ª edição. 2020

[211] WARREN, Samuel D. BRANDEIS, Louis D. **"The Right to Privacy".** Harvard Law Review. Vo. IV, December 15, 1890, No. 5. *Disponível em* https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[212]These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in pre- venting publication, is merely an instance of the enforcement of the more general right of the individual to be let alone WARREN, Samuel D. BRANDEIS, Louis D. **"The Right to Privacy".** Harvard Law Review. Vo. IV, December 15, 1890, No. 5. Disponível em https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html" P 205

[213]"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone. " 4 Instantaneous photographs and news- paper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that " what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons ; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. WARREN, Samuel D. BRANDEIS, Louis D. **"The Right to Privacy".** Harvard Law Review. Vo. IV, December 15, 1890, No. 5. *Disponível em* https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html" 196 p.

Apesar das profundas alterações culturais, sociais e comportamentais sofridas pela sociedade desde o século XIX, bem como das evoluções da tecnologia e do instituto da privacidade, o risco à violação desse direito está maior do que nunca, pois envolve o controle, estatal ou do mercado, sobre a vida privada. Nas últimas décadas, a academia debate sobre este tema[214], que está intimamente ligado às cidades inteligentes, como será analisado após o estudo conceitual da privacidade.

A noção de privacidade cria uma relação de oposição entre o indivíduo e a sociedade. Este significado tem origem no desenvolvimento do conceito de liberdade, ligado à proteção da propriedade e da autonomia privada[215].

Warren e *Brandeis* desvinculam o direito à privacidade do direito à propriedade, trazendo-o para a esfera pessoal [216]. Assim, a privacidade passou a ser considerada como um direito da personalidade[217].

Após a criação do "*right to be let alone"*, foi atribuído ao conceito de privacidade diferentes definições que atendessem a outras necessidades:

> *...o direito de controlar a maneira na qual os outros utilizam as informações a nosso respeito (A. Westin) ...a proteção de escolhas da vida contra qualquer forma de controle público e estigma social (L.M.Friedman)...a reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto (J. Rosen)... o direito de manter o controle sobre suas próprias*

---

[214] Sobre a privacidade nas tecnologias disruptivas, recomenda-se: ZUBOFF, Shoshana.. **A era do capitalismo de vigilância. A luta por um futuro humano na nova fronteira do poder.** Editora Intrínseca LTDA. 1ª edição digital. 2021.

[215] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020. 90 p.

[216]**"**These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in pre- venting publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed - and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.*"* WARREN, Samuel D. BRANDEIS, Louis D. **"The Right to Privacy".** Harvard Law Review. Vo. IV, December 15, 1890, No. 5. *Disponível em* https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html 205 p.

[217] "Portanto, em uma primeira acepção, os "direitos de personalidade" são projeções do ser humano e cuja tutela está amparada no valor fundamental da pessoa humana, diferenciando-se, neste sentido, da concepção de direito real (sujeito-coisa)." LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. De acordo com a lei geral de proteção de dados (lei N 13.709/2018 e as alterações da lei n.13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alterações do CDC (PL.3514/2015)** Editora Almedina. São Paulo. 2020. 83 p.

> *informações e de terminar a maneira de construir a sua própria esfera particular (R. Rodotá)*[218]

O surgimento da sociedade informacional, o qual pressupõe a coleta e o armazenamento de informações pessoais, criou a necessidade de desenvolver a natureza da privacidade. Com efeito, a tutela da privacidade passou a garantir ao indivíduo o direito *de controlar, identificar e interromper o fluxo de informações*[219] sobre a sua pessoa [220].

A proteção dos dados pessoais decorreu da evolução do direito à privacidade. Durante o período de desenvolvimento sobre a natureza jurídica da privacidade, os instrumentos legislativos europeus adotavam um conceito abrangente de privacidade que englobava a proteção dos dados pessoais.

Desde 1970, a República Federal da Alemanha possuía uma lei sobre a proteção de dados pessoais, chamada *Land de Hesse*, que teve como destaque na sua criação o jurista grego *Spiros Simitis.* Nesta época, os alemães já detinham uma cultura de proteção de dados pessoais, adotando estruturas administrativas que observavam esse direito[221]

Em se tratando de UE, foi só a partir da Carta de Direitos Fundamentais da União Europeia do ano 2000 que houve o reconhecimento do direito à proteção dos dados pessoais como um direito de personalidade autônomo. Este diploma é considerado o último ponto da longa evolução do direito à privacidade, separando-o da proteção de dados pessoais[222].

Além de serem tutelados por dispositivos diferentes,[223] a privacidade e a proteção de dados pessoais são direitos distintos quanto aos seus objetos. A privacidade visa proteger o

---

[218]RODOTÁ, Stefano. ***A vida na sociedade de vigilância. A privacidade hoje.*** Editora Renovar. 2008. 15 p.

[219]"Preliminarmente, ressalta a distinção entre "dados e "informação". Entende-se por "dado" uma informação latente. A "informação", por outro lado, é a interpretação ou representação que se extrai do dado. ...Pode-se informar que o dado é uma fonte da qual se extrai uma informação, ou seja, a informação está contida em um ou em vários dados, dos quais ela é extraída ou inferida. Em síntese "a informação é a elaboração de um dado*"*. LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. De acordo com a lei geral de proteção de dados (lei N 13.709/2018 e as alterações da lei n.13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alterações do CDC (PL.3514/2015)** Editora Almedina. 2020. São Paulo. 92 p.

[220] LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. De acordo com a lei geral de proteção de dados (lei N 13.709/2018 e as alterações da lei n.13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alterações do CDC (PL.3514/2015)** Editora Almedina. 2020. São Paulo. 89 p.

[221]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020. 167 p.

[222]RODOTÁ, Stefano. ***A vida na sociedade de vigilância. A privacidade hoje.*** Editora Renovar. 2008. 16 p.

[223] A exemplo da Carta dos Direitos Fundamentais da União Europeia, o seu artigo 7º dispõe sobre o direito pela vida familiar e privada, enquanto o artigo 8º trata, de forma específica, da proteção dos dados pessoais. EUROPA PARLIAMENT. **Carta dos Direitos Fundamentais da União Europeia.** Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf

indivíduo de intervenções exteriores, enquanto a proteção de dados pessoais tutela a dinâmica dos dados pessoais nas suas várias formas de tratamento[224].

Dos objetos de tutela, ainda se extrai outra diferença entre os direitos à privacidade e à proteção de dados pessoais. O primeiro é estático e negativo e o segundo é dinâmico e se estrutura em regras de tratamento como a coleta de dados pessoais, o seu armazenamento e a sua transmissão[225].

A diferença prática dos dois direitos está na circulação dos dados. Na privacidade, há uma proibição absoluta do acesso e da circulação dos dados pessoais, enquanto que na proteção dos dados pessoais existe a regulação dessa prática a partir de regras que a condicionam, como, a portabilidade, o compartilhamento e o tratamento de dados pessoais limitado à finalidade informada pelo agente.

Depois de décadas de discussões, a privacidade foi aceita como um direito de personalidade em vários países, a exemplo dos EUA, que, mesmo de forma tardia, reconheceu a privacidade como um direito protegido pela Constituição Americana [226]. No entanto, definir a delimitação do direito à privacidade é um desafio, pois sua limitação é determinada pelos valores de cada ser humano que vive em sociedade.

A diversidade de entendimento sobre a delimitação da privacidade é um problema para as cidades inteligentes, uma vez que muitas tecnologias inseridas nas cidades são de origem estrangeira. Geralmente, a empresa de TIC desenvolve seus produtos e serviços tecnológicos de acordo com a concepção de privacidade do seu lugar de origem, buscando uma conformidade com as leis de privacidade do país onde a organização foi criada.

No entanto, o ideal seria uma padronização internacional do conceito e da delimitação da privacidade, mas, sabe-se que isto é uma utopia. Uma solução mais palpável é a criação de produtos e serviços que ofereçam opções de controle pelo titular de dados pessoais, com diferentes graus de proteção sobre a sua privacidade.

Todavia, a necessidade de encontrar um conteúdo comum para a privacidade, capaz de garantir um grau mínimo de proteção desse direito em lugares distintos, é fundamental para situações como, por exemplo, de uma empresa estrangeira que utiliza informações sobre a

---

[224] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados**. Revista dos Tribunais. 2ª edição. 2020. 41 p.

[225] LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. De acordo com a lei geral de proteção de dados (lei N 13.709/2018 e as alterações da lei n.13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alterações do CDC (PL.3514/2015)** Editora Almedina. 2020. São Paulo. 91 p.

[226] DONEDA, ***Danilo. Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados***. Revista dos Tribunais. 2ª edição. 2020 94 p.

genética do titular dos dados. Em casos como este, que vão além do controle do titular dos dados sobre as informações privadas que ele gostaria ou não que fossem expostas para a sociedade, existe a necessidade real de criar uma harmonização sobre a privacidade e o tratamento de dados pessoais para diversos países[227].

Tratar sobre privacidade em cidade inteligente é um assunto ainda mais complexo, pois o elemento tecnológico inserido na relação entre o indivíduo e a sociedade está mais poderoso do que nunca. Este ambiente, além de ter uma capacidade imensurável de absorver dados, inclusive pessoais, consegue penetrar na esfera íntima do indivíduo sem que ele perceba.

A tecnologia atual tem instrumentos capazes de influenciar o pensamento humano, interferindo na sua liberdade de escolha. Desse modo, o desafio é criar um significado de direito à privacidade atual que abranja todas as situações das quais este direito não seja violado no contexto de cidade inteligente.

Um sentido importante de privacidade na implantação de *smart city* consiste na defesa da pessoa humana contra o exterior, em prol dos direitos à autonomia, à cidadania e dos direitos de liberdade[228]. A proteção da privacidade na cidade inteligente deve oferecer condições ao cidadão de desenvolver a sua personalidade, deixando-o livre da interferência externa do controlador dos dados, seja ele o Estado ou o mercado privado, que não terá conhecimento nem influência sobre a sua intimidade e sobre as suas escolhas.

Outra concepção importante da privacidade para a cidade inteligente é o direito do cidadão de manter o controle sobre as suas próprias informações, determinando as modalidades de construção da própria esfera privada. Inclusive, este significado de privacidade se desenvolveu e hoje se transformou em um fundamento da LGPD constante no artigo 2, inciso II, chamado de autodeterminação informativa[229].

A criação e a consolidação da autodeterminação informativa dependem da existência de uma infraestrutura tecnológica que capacita o indivíduo para ter o controle de suas

---

[227] DONEDA*, Danilo.* **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020. 94 – 95 p.

[228] DONEDA, Danilo*.* **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020. 96 p.

[229] "A autodeterminação informacional consiste, em suma, na perspectiva de que o indivíduo deve controlar (autodeterminar) os seus dados pessoais (informações pessoais: autodeterminação informacional), exigindo-se, por isso, o consentimento do titular das informações pessoais para que elas sejam coletadas, processadas e compartilhadas*."* BIONI, Bruno Ricardo. **Proteção de Dados- Contexto, narrativas e elementos fundantes** BIONI Data Privacy Specialist. 151 p.

informações[230]. Portanto, tão importante quanto a arquitetura jurídica para o exercício da privacidade é a arquitetura tecnológica, que pode fortalecer esse direito ou enfraquecê-lo[231].

Inclusive, em estudo técnico sobre a limitação tecnológica, foi diagnosticado o risco à privacidade em sistemas de *smart city* e em produtos tecnológicos desenvolvidos para cidades por conta da falta de transparência do tratamento de dados pessoais. Além disso, a assimetria de informação e a falta de segurança dos dados pessoais em cidades inteligentes também foram citadas neste estudo.[232]

Especificamente, a ausência de informação sobre como é feito o tratamento de dados pessoais, levanta suspeitas quanto ao seu uso. Sem a consciência do cidadão sobre quais são os dados pessoais coletados, como eles são tratados, quais são as finalidades do tratamento e com quem os dados pessoais são compartilhados, dificilmente uma sociedade consciente da importância da proteção dos dados pessoais e da privacidade será a favor da implantação massiva de tecnologia nos ambientes urbanos.

A cidade inteligente permite que os dados pessoais sejam facilmente acessíveis em áreas públicas e combina as três tecnologias que possuem o maior potencial para ameaçar o direito à privacidade, que são a *Internet of Things* (IoT), o *big data* e o *cloud*[233]. Além dessas tecnologias, o blockchain e a Inteligência Artificial também foram citados em pesquisas como tecnologias que colocam em risco a privacidade do cidadão em ambiente tecnológico urbano[234].

Os dispositivos de IoT foram planejados para funcionar de forma contínua e imperceptível. Os seus sensores foram programados para captar a rotina e os desejos do usuário, com o propósito de lhe oferecer um serviço personalizado como, temperatura e iluminação de um ambiente privado[235]ou informações diversas sobre as situações das rodovias[236] .

---

[230] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados**. Revista dos Tribunais. 2ª edição. 2020 P 10

[231] BIONI, Bruno Ricardo. **Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet.** São Paulo: Faculdade de Direito da Universidade de São Paulo, 2016, 211 p.

[232]SHARIF, Al Sharif; POKHAREL, Shaligram. **Engineering Advance. Smart City Dimensions and Associated Risks.** Sustainable Cities and Society (SCS) international journal. ScienceDirect Disponível em: https://www.sciencedirect.com/journal/sustainable-cities-and-society 1 p.

[233] EDWARDS, Lilian. **Privacy security and data protection in smart cities a critical EU law perspective** Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711290 1.p

[234]SHARIF, Al Sharif; POKHAREL, Shaligram. **Engineering Advance. Smart City Dimensions and Associated Risks.** Sustainable Cities and Society (SCS) international journal. ScienceDirect Disponível em: https://www.sciencedirect.com/journal/sustainable-cities-and-society

[235]EDWARDS, Lilian. **Privacy security and data protection in smart cities a critical EU law perspective** Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711290 17 p.

[236]DTG. **Qué es DTG 3.0.** Disponível em: https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/dgt-3.0/

Estudo técnico sobre a implantação de sensores de IoT em ambientes urbanos afirma que a proteção à privacidade do cidadão é um desafio. Além do mais, é sabido que a privacidade é indispensável para o desenvolvimento de políticas urbanas baseadas em sensores e câmaras de videovigilância[237].

Portanto, nos tempos atuais, há uma preocupação crescente da indústria inteligente baseada em IoT, com o desenvolvimento de produtos e serviços que estejam em conformidade com as regras de privacidade. A criptografia e a criação de modelos de controle e de novas arquiteturas de segurança são algumas das soluções pelas quais a indústria de IoT se apega para garantir a privacidade exigida pela legislação[238].

Já o *big data,* que talvez seja a tecnologia mais comum em cidades inteligentes, tornou possível a inferência de dados em uma escala massiva e a um baixo custo. Smartphones e outros dispositivos geram cada vez mais dados que são difíceis de proteger, deixando lastros sobre os hábitos dos usuários. Essas informações são passíveis de vigilância, permitindo a identificação e o monitoramento do indivíduo[239].

A análise de *Big data* também tem o potencial de criar informações. Um exemplo são sensores em carros que fornecem dados sobre o veículo, mas que também servem para identificar padrões de comportamento de direção das pessoas, informando o perfil do motorista para o seguro[240].

Outro perigo do *big data* para a privacidade é a possibilidade de reaproveitar os dados pessoais coletados para finalidades diferentes da original. Inclusive, o *big data* pode associar dados entre dois grandes bancos de dados, mesmo que estes bancos sejam de dados anonimizados, para identificar pessoas. Um exemplo dessa prática é a associação do banco de dados *footfall* com o banco de dados CCTV.

Por fim, tem-se a tecnologia *cloud* utilizada em cidades inteligentes. Os dados em nuvem são armazenados e processados de forma distribuída, ou seja, através de vários backups

---

[237] D AMICO, Gaspare; L ABBATE, Pasqua; LIAO, Wenjie; **Understading Sensor Cities: Insights From Technology Giant Company Driven Smart Urbanism Practices.** MDPI Disponível em: https://www.mdpi.com/1424-8220/20/16/4391.. 14 p.

[238] VORAKULPIPAT, CHALEE; KO, RYAN K. L; LI, QI, MEDDAHI, Ahmed. **Security and privacy in Smart City.** August 2021. HINDAWY. Security e communication Networks. Disponível em: https://www.hindawi.com/journals/scn/2021/9830547/

[239] KITCHIN, Rob. **Data Driven, networked urbanism. The Programmable City** WP 14. Agosto de 2015. Disponível em: http://www.spatialcomplexity.info/files/2015/08/SSRN-id2641802.pdf . 18 p.

[240] INTERNATIONAL COMMISSIONER'S OFFICE. **Big Data and Data Protection**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220 12 p.

ou processadores, sendo que cada equipamento pode estar em um local diferente, muitas vezes em países distintos.

Nesse caso, têm-se dois problemas jurídicos internacionais que são o conceito de privacidade adotado para cada situação e quais sãos as garantias para a proteção desse direito. A escolha dessa celeuma fica entre os entendimentos do país gerador dos dados pessoais e do país que os armazenam ou os processam, a exemplo do novo acordo, realizado em julho de 2023, entre a Europa e os EUA sobre a transferência e o compartilhamento de dados pessoais[241].

Em 2021, *a European Union Agency for Cybersecurity* (ENISA) publicou um relatório sobre segurança em *cloud* para serviços de saúde, com o objetivo de fornecer práticas de segurança para esse setor, incluindo aspectos relevantes de proteção de dados.[242] Este relatório pontuou os desafios de proteção de dados para o *ambiente em cloud.*

O primeiro desafio citado foi a falta de interesse do prestador de serviços de saúde de aplicar as técnicas de privacidade desde a concepção da tecnologia, item a ser estudado no capitulo dois desse trabalho. Outro desafio é a falta de estrutura de governança de dados para melhorar a compreensão do tipo de dado coletado bem como de qual tratamento é o adequado para aquele conjunto de dados[243].

Em seguida, o relatório cita como um desafio técnico a eliminação eficaz de dados em *cloud*. A garantia da portabilidade dos dados também é citada como um desafio dos sistemas de cloud[244].

Por último, o relatório destaca a dificuldade em implementar a criptografia no serviço de armazenamento em cloud. A complexidade desse processo reside na inserção da criptografia em todos os canais de transferência e armazenamento de dados, tanto a nível de cliente como do servidor[245].

Por fim, os aplicativos de *smart city* que utilizam IoT, *big data* e computação em nuvem têm sofrido problemas com vazamento de informações confidenciais e sensíveis. A privacidade em sistemas integrados de *smart city* nas cidades tem sido ponto de preocupação dos

---

[241] CNBC. **Europe and the U.S. finally agree a landmark data-sharing pact - -and it's already under threat.** 12/07/2023. Disponível em: https://www.cnbc.com/2023/07/12/eu-and-us-agree-new-data-sharing-deal-what-is-it-and-why-it-matters.html

[242] EUROPEAN UNION AGENCY FOR CYBERSECURIT. **Cloud Security for Healthcare Services.** 2021. Disponível em: Yhttps://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services.

[243] EUROPEAN UNION AGENCY FOR CYBERSECURIT. **Cloud Security for Healthcare Services.** 2021. Disponível em: Yhttps://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services 18 p.

[244] EUROPEAN UNION AGENCY FOR CYBERSECURIT. **Cloud Security for Healthcare Services**. 2021. Disponível em: Yhttps://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services 18- 19 p.

[245] EUROPEAN UNION AGENCY FOR CYBERSECURIT. **Cloud Security for Healthcare Services.** 2021. Disponível em: Yhttps://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services. 19 p.

desenvolvedores da tecnologia, pois as técnicas atuais de privacidade ainda possuem falhas de latências, eficiência e desempenho[246].

Diante de todos esses problemas supracitados, entende-se como fundamental mais estudos sobre a privacidade nas cidades inteligentes. Conforme explicitado no início deste item, o objetivo deste estudo é contextualizar os diversos riscos à violação da privacidade dos cidadãos no ambiente tecnológico urbano, expondo a importância deste assunto e a ausência de estudos específicos em território brasileiro.

2.4. Questões relativas aos agentes de tratamento na cidade inteligente

Preambularmente, este item conceitua os *agentes de tratamento*, as características que os definem e os seus deveres perante o sistema de proteção de dados pessoais brasileiro. Após, utiliza exemplos hipotéticos de implantação da tecnologia *smart city* em cidade brasileira para tratar de algumas questões de identificação de agentes de tratamento neste ambiente. Finalmente, pontua os benefícios para a proteção de dados pessoais em *smart city* quando da identificação e acesso fáceis do agente de tratamento.

No Brasil, o termo *agentes de tratamento* se refere a sujeitos que estão envolvidos com as operações de dados pessoais[247], seja na tomada de decisão, seja na execução das operações[248]. Porém, nem todo sujeito que se relaciona com tratamento de dados pessoais é considerado um agente de tratamento.

Um exemplo é o encarregado (conhecido no estrangeiro como *data protection officer* - DPO)[249] que, mesmo sendo regulado no capítulo VI da LGPD, não se enquadra no conceito legal de agente de tratamento[250]. No entanto, isso não diminui a importância do DPO, figura

---

[246] PANDYA, Sharnil; SRIVASTAVA, Gautan; JHAVERI, Rutvij e outros. **Federal Learning for smart cities: A comprehensive survey.** Susteinable Energy Technologies and Assessments. Elsevier. 2022. Disponível em: http://www.elsevier.com/locate/seta. 9 p.

[247] Em seu artigo 5, inciso X, a LGPD traz um rol exemplificativo de operações realizadas com dados pessoais: "X - tratamento: toda operação realizada com dados pessoais, **como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração**;" **grifo e negrito nosso.**

[248] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller> 7 - 8 p.

[249] Segundo o artigo 5º da LGPD, o conceito de encarregado: "VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)**."**

[250] "Apesar de também regulado no mesmo capítulo da LGPD (Capítulo VI: Dos Agentes de Tratamento de Dados Pessoais), o encarregado pelo tratamento desses dados (internacionalmente denominado *data protection officer* – DPO) não se inclui no estrito conceito legal de agentes de tratamento. Melhor seria, então, que o referido capítulo

que deve estar, obrigatoriamente, presente na implantação de *smart city* no ambiente urbano e, portanto, merece menção neste tópico antes de adentrar em seu objeto.

O encarregado de proteção dos dados pessoais é o responsável por estabelecer a comunicação entre a empresa, o titular e a ANPD. Além de receber as comunicações, o DPO deve prestar esclarecimentos e adotar providências[251].

Este profissional serve de ponto conciliador entre as partes interessadas, podendo evitar conflito entre elas. Ademais, o encarregado tem o papel de monitorar o tratamento de dados pessoais, verificando a sua conformidade com a legislação[252].

A LGPD classifica como *agentes de tratamento* o controlador e o operador, trazendo também as suas definições.[253] A partir de uma simples leitura do seu artigo 5º, verifica que qualquer pessoa, natural ou jurídica, de direito público ou privado, pode ser classificada como agente de tratamento de dados pessoais.

Apesar das semelhanças entre as figuras do controlador e do operador, eles possuem alguns deveres distintos. Estabelecer a diferença clara entre o controlador e o operador é fundamental para a aplicação da lei, pois são conceitos funcionais que determinam a responsabilidade de acordo com os papeis por eles exercidos na prática [254].

As obrigações legais relacionadas aos direitos e garantias do titular de dados são, majoritariamente, direcionadas ao controlador. Portanto, na maioria dos casos, ele é o responsável pela proteção dos dados pessoais [255].

---

fosse rotulado de forma mais ampla, como algo do tipo: "Principais sujeitos envolvidos no tratamento de dados pessoais". Existem razões técnicas para a exclusão do DPO do conceito de agentes de tratamento, mas não vem ao caso abordá-las neste estudo, pois isto seria um desvio do tema proposto. Basta o sucinto registro já efetuado." PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>. 9 p.

[251] "Art. 41. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares." Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

[252] QUEIROZ, Renata Capriolli Zocatelli, **Encarregado de Proteção de Dados Pessoais- DPO. Regulamentação e Responsabilidade Civil**. Editora Quartier Latin do Brasil. 2022. 80 p.

[253]O artigo 5º da LGPD traz as definições: "IX - agentes de tratamento: o controlador e o operador; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador."

[254] UNIÃO EUROPEIA. European Data Protection Board. **Guideline nº 07/2020: on the concepts of controller and processor in the GDPR.** Brussels: 02 Sep. 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_pt> 3 p..

[255] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>. 8 p.

A título de exemplo, a finalidade do tratamento, ponto estudado em tópicos anteriores e muito importante para a proteção de dados pessoais em implantação de tecnologia *smart city,* é definida pelo controlador. Além disso, o controlador é quem indica o encarregado pelo tratamento dos dados e elabora os relatórios de impacto, ambos essenciais para a implantação de *smart city* no ambiente urbano, como é estudado em tópicos posteriores.

A diferença principal entre os agentes é a atribuição decisória do controlador sobre as operações de tratamento dos dados. Esta característica torna a sua figura essencial, pois não existe tratamento de dados pessoais sem que haja um sujeito que tomou as decisões sobre este tratamento[256].

Já o operador é o responsável por realizar as operações de tratamento de dados pessoais, executando as decisões recebidas pelo controlador. Mesmo em casos que o operador age sem a autorização expressa, ele não muda de figura se a sua ação era necessária para cumprir alguma ordem direta do controlador[257].

Porém, na prática, determinar qual decisão do operador é ou não necessária pode ser complicado. Se a ANPD considerar que o operador tomou uma decisão que apenas o controlador poderia determinar, ele responde, de forma solidária com o controlador, por eventuais danos causados ao titular dos dados[258].

A identificação dos agentes de tratamento também se torna trabalhosa quando há extensas cadeias de tratamento de dados, com dois ou mais controladores e vários operadores. Em alguns casos, diferenciar o controlador do operador é uma tarefa complexa, especialmente quando uma entidade pode ser controladora em uma operação de tratamento de dados e operadora em outra.

---

[256] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller> 13 p.

[257] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>. 14 p.

[258]"Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;" Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

É comum haver extensas cadeias de tratamento de dados em ambientes tecnológicos urbanos. Como opção didática, é utilizado o exemplo de aplicação de *smart cty*, qual seja, *The European Institute for Innovation through Health Data (I~HD)* [259].

Para isso, considera a situação hipotética na qual o programa *I~HD* foi implantado no Brasil e trata apenas dados pessoais de cidadãos brasileiros no território nacional. Nestas condições, todo e qualquer tratamento de dados pessoais do programa fica sob a égide do sistema de proteção de dados brasileiro.

Este programa, que utiliza tecnologias TIC como *big data* e IA, tem o objetivo de reutilizar os dados pessoais dos pacientes para o desenvolvimento da área da saúde [260]. Além de promover a qualidade dos sistemas de saúde eletrônicos (em inglês *Eltronic Helth Record* – EHR), o *I~HD* criou padrões de interoperabilidade ente os EHR, interligando-os.

As entidades registradas no programa, como hospitais e clínicas de saúde, coletam manualmente e depositam os dados pessoais no seu EHR, conforme as orientações e diretrizes do *I~HD*. Após, as organizações inscritas no programa e autorizadas acessam os bancos de dados, utilizando-os para diversas finalidades, como, para desenvolver novos produtos médicos, melhorar a qualidade do tratamento personalizado, realizar investigações clínicas e pesquisas acadêmicas.

Esse ecossistema de dados de saúde possui vários *players,* gerando um ambiente propício para a criação de cadeias de tratamento de dados pessoais de diferentes tamanhos. A seguir, uma imagem explicativa fornecida pela *I~HD,* que mostra a variedade de organizações envolvidas no ecossistema de saúde do programa.

[259]THE EUROPEAN INSTITUTE FOR INNOVATION THROUGH HEALTH DATA. **Trustworthy Health ICT Systems**. Disponível em*:* https://www.i-hd.eu/trustworthy-health-ict-systems/

[260] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for Quality.** Disponível em: https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality 1 p.

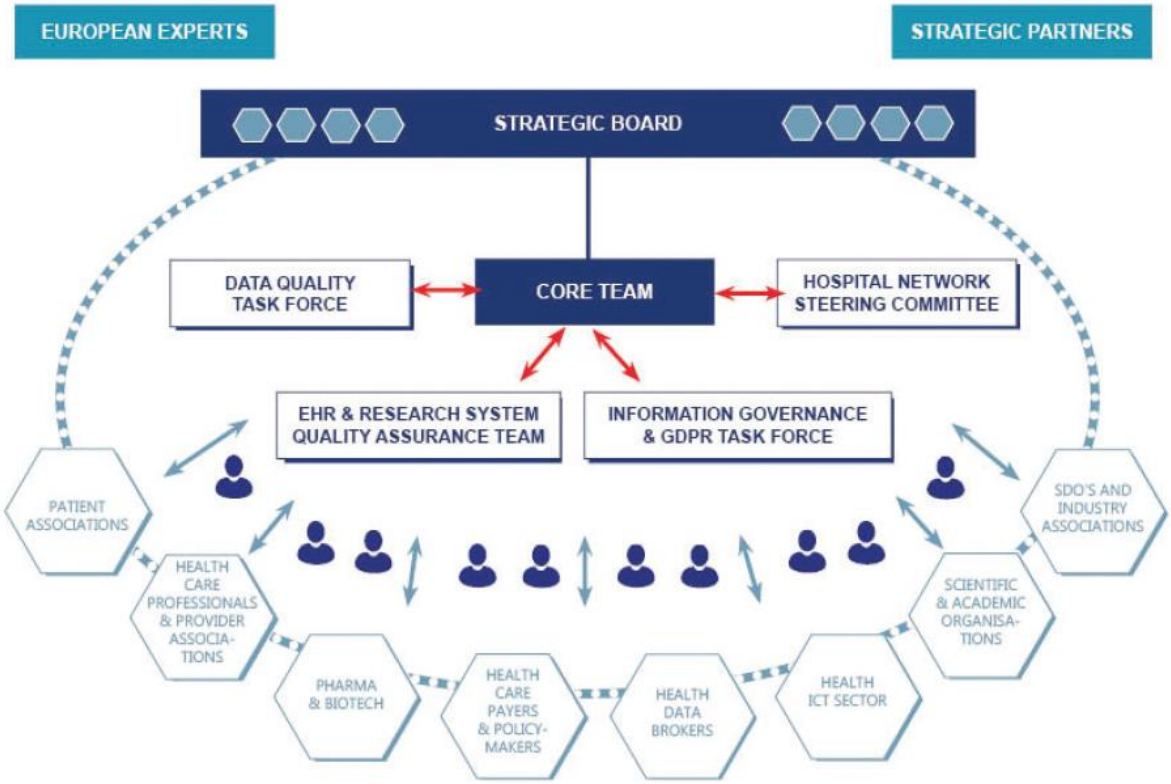

Figura 2: Ecossistema de saúde do I~HD[261]

Extrai-se da figura 2 que empresas de TIC, hospitais, clínicas, associações, universidades e indústrias participam do ecossistema da *I~HD*. Todos eles podem ser caracterizados como agente de tratamento, conforme os conceitos extraídos dos incisos do artigo 5º da LGPD.

Inicialmente, imagine um hospital inscrito como fornecedor do seu EHR para o programa *I~HD*. Porém, esse hospital terceiriza o serviço de coleta e transferência dos dados do seu sistema eletrônico de saúde para uma empresa privada de TIC.

Neste caso, o hospital é o controlador e a empresa privada é a operadora, mesmo que aquele não tenha como atividade principal o uso da tecnologia. O hospital é quem toma as principais decisões do tratamento de dados pessoais de seus pacientes e a empresa de TIC executa as operações, a comando do controlador.

Agora, suponha-se que a empresa de TIC contratada pelo hospital, além de prestar serviços relacionados com EHR, participa do programa *I~HD* para coletar dados pessoais com

[261] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for Quality.** Disponível em https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality 3 p.

o propósito de desenvolver aplicativos de saúde. Aqui, a empresa de TIC se encaixa em operadora no primeiro caso e controladora no segundo.

Em outra situação, uma clínica de saúde fornece dados pessoais dos seus pacientes para o programa e, ao mesmo tempo, adere o *I~HD* para coletar dados com a finalidade de desenvolver um tratamento específico. Neste caso, a clínica é considerada controladora em dois tratamentos de dados pessoais distintos, cada um com as suas obrigações.

Em uma cadeia de tratamento de dados extensa, é possível encontrar a figura do suboperador, que é um agente de tratamento contratado pelo operador original para realizar parte ou todo o serviço de tratamento. Neste caso, a ANPD considera que ambos são operadores[262] e, portanto, respondem pelos deveres impostos pelo sistema de proteção de dados pessoais brasileiro.

Voltando ao exemplo hipotético do programa *I~HD* supra mencionado, suponha-se que a empresa de TIC contratada pelo hospital transfere a prestação do serviço para outra empresa. Para a ANPD, tanto a operadora originária como a suboperadora serão consideradas operadoras.[263]

Além das situações de identificação de agentes de tratamento de dados relatadas, é preciso atentar para as espécies de controladores em ambiente tecnológico urbano, que podem acarretar consequências jurídicas diversas. A título de exemplo, quando há dois ou mais controladores que tomam decisões sobre um mesmo banco de dados, é preciso analisar a decisão de cada controlador.

Se os controladores tomam as decisões em comum acordo e tais decisões não podem ser tomadas sem a participação de todos eles, tem-se a figura do controle conjunto (*joint controllership*). Entretanto, se cada controlador toma as suas próprias decisões sobre o mesmo banco de dados e estas decisões não interferem nos demais controladores, então há o controle independente (*independente controllership*)[264].

---

[262] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>. 16 p.

[263] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>. 16 p.

[264] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller> 20 p.

Suponha-se, no exemplo hipotético do *I~HD,* haja um banco de dados que armazena todas as informações de cada EHR, ficando estabelecido via contrato que cada organização fornecedora de dados pessoais deve analisar e validar a operação de transferência dos dados antes de armazená-los no sistema. Neste exemplo, há o controle conjunto, uma vez que está caracterizada a necessidade da participação de todos os controladores nas tomadas de decisão de um mesmo banco de dados.

Continuando na mesma hipótese, os centros de pesquisas de saúde que utilizam os dados pessoais podem servir de exemplo de controle independente. Cada centro de pesquisa decide quais dados pessoais serão tratados e a finalidade pelo qual serão utilizados, como, por exemplo, para a investigação de uma determinada doença, realizando o tratamento de dados pessoais conforme os seus interesses e sem influência de outro controlador.

Outra questão importante para fins práticos é a possibilidade de o operador assumir voluntariamente deveres inerentes ao controlador. Como a LGPD não proíbe esta possibilidade, os agentes de tratamento interessados podem realizar este acordo via contrato (denominado *data processing agreement* – DPA)[265]. .

No Brasil, ainda há uma situação peculiar para a identificação de controlador pessoa jurídica de direito público, que advém da sua organização administrativa. Especificamente, na hipótese de desconcentração administrativa, da qual não há o surgimento de uma pessoa jurídica, mas a criação de órgãos públicos que serão subordinados a entidade administrativa do qual fazem parte[266].

Neste caso, existe uma distribuição interna de competências decisórias entre diferentes órgãos públicos de uma mesma entidade. Para fins de proteção de dados pessoais, a ANPD considera que o controlador será a entidade da qual o órgão público que tomou a decisão faz parte, atribuindo àquele as responsabilidades legais das decisões tomadas pelo órgão[267].

Todavia, por conta da desconcentração administrativa, a ANPD considera que a LGPD confere ao órgão público as atribuições de controlador que desempenha funções em nome da pessoa jurídica de direito público que ele integra. Portanto, o órgão público deve cumprir com os deveres atribuídos ao controlador, além de ter um encarregado responsável por realizar a

---

[265] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller> 7 – 8 p.

[266] OLIVEIRA, Rafael Carvalho Rezende. **Curso de Direito Administrativo**. 6ª ed. 2018. Editora Método. 79 p.

[267] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais.** Brasília: mai. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf>. 8 p.

comunicação com a pessoa jurídica de direito público controladora, os titulares dos dados e a ANPD[268].

Em ambiente de *smart city*, cita-se como exemplo o Smart Sampa, programa de videomonitoramento com finalidade de aprimorar serviços públicos, especialmente a segurança.[269] Na hipótese de realização de tratamento de dados pessoais por um órgão público vinculado à prefeitura de São Paulo, este será o controlador e aquele realizará as atribuições do controlador, estabelecidas pela LGPD.

A identificação clara do agente de tratamento, bem como a sua fácil comunicação são condições determinantes para o sucesso da implantação de *smart city* em ambiente urbano. O agente de tratamento de fácil acesso pode garantir direitos do titular de dados como os relacionados a pedidos de portabilidade e de explicação sobre o tratamento de dados pessoais.

Ademais, o estabelecimento de redes de comunicação com o controlador facilita na manutenção da base legal de tratamento, a ser estudado *a posteriori*, para, por exemplo, o pedido de consentimento do titular na utilização de seus dados pessoais para finalidade diversa da comunicada inicialmente[270]. Ainda, o agente de tratamento identificado pode ser fiscalizado, e, se for o caso, responsabilizado por danos ao titular.

Além de outros benefícios técnicos e jurídicos de proteção de dados pessoais, o controlador de fácil identificação e acesso também serve de argumento para diminuir a desconfiança da população quanto à implantação de *smart city.* Em cidades com culturas mais conservadoras sobre o compartilhamento dos dados pessoais, o trabalho de convencer os cidadãos tende a ser uma tarefa árdua[271].

---

[268] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais.** Brasília: mai. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf>. 9 p.

[269] PREFEITURA DE SÃO PAULO. **Prefeito assina contrato para o início do Smar tampa, maior programa de videomonitoramento da cidade com até 40 mil câmeras.** Disponível em: https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2

[270] Segundo o artigo 7º e 8º da LGPD: "Art. 7. (...). § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular".

[271] Um dos casos mais emblemáticos é o fracasso do programa Sidewalk Toronto. Houve uma pressão popular contra a implantação de tecnologia smart city na cidade de Toronto, Canadá, com listas sobre a preocupação com a privacidade e os dados pessoais. Vide WYLIE, Bianca. **Civic Tech: A list of questions we'd like Sidewalk plan for ist Toronto Project.** 30/10/2017. Torontoist. Disponível em: https://torontoist.com/2017/10/civic-tech-list-questions-wed-like-sidewalk-labs-answer/

Identificar os controladores e os operadores em uma cidade inteligente nem sempre é uma tarefa fácil, especialmente quando há uma vasta cadeia de tratamento de dados com a participação de muitos agentes. Por conta disso, a fiscalização do tratamento de dados em uma cidade inteligente é complexa e pode deixar a entidade fiscalizadora sobrecarregada.

Neste sentido, destaca-se a alteração no regulamento europeu sobre a forma de fiscalização de tratamento de dados[272], modelo este adotado pela LGPD (*accountability*)[273]. As exigências impostas anteriormente à alteração, como registros públicos e comunicações prévias às autoridades nacionais de proteção de dados, foram substituídas pelo controle dos próprios agentes de tratamento, agora responsáveis por assegurar que o tratamento de dados seja realizado em conformidade com a lei[274].

Deste modo, presume-se a boa fé e a conformidade jurídica do controlador, deixando que eventual fiscalização da autoridade competente seja realizada posteriormente. O *accountability* transfere ao controlador o ônus de comprovar que o tratamento de dados pessoais está de acordo com as exigências legais, caso seja indagado pelo titular dos dados, autoridades públicas ou outro sujeito legitimado[275]

Entende-se que a mudança no modelo de fiscalização no tratamento de dados pessoais traz, para o caso específico de cidade inteligente, benefícios à inovação tecnológica como a desburocratização estatal para o surgimento de empresas de TIC, e a desoneração do Estado quanto a custos financeiros e de mobilização de pessoal.

Por outro lado, questiona-se a respeito do investimento dos agentes de tratamento em cidades inteligentes na criação ou adoção de tecnologias que priorizam a proteção de dados pessoais, bem como na realização de treinamento do pessoal envolvido nas operações de tratamento.

---

[272] Segundo o GDPR *artigo "*5. 2 2.O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo («responsabilidade»). Art 24. I 1.Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades".

[273] O artigo 6º da LGPD, acolheu o princípio do *accountability* europeu: "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"

[274] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>. 5 p.

[275] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller> 5 p.

Outra preocupação está na forma como os entes federativos, especialmente os municípios, irão se organizar para atender às exigências impostas pelo sistema de proteção dos dados pessoais sob os seus complexos bancos de dados. Por ser constituído de vários órgãos, o município pode ter diversos problemas, tais como, incidentes de segurança, falta de padronização de tratamento dos dados pessoais entre os seus órgãos e dificuldade de garantir que o titular exerça o seu direito à portabilidade dos seus dados.

Por fim, a relação do município com terceiros prestadores de serviços públicos também é um tema interessante para investigações futuras de proteção dos dados pessoais na implantação de *smart city.* Há experiência estrangeira sobre contrato de parceria público-privada de implantação de *smart city* com regras obscuras de compartilhamento de dados pessoais, falta de transparência no tratamento e ausência de informações a respeito da identidade dos controladores de sensores em IoT.[276]

Para evitar esses problemas, primeiramente, é fundamental a promoção de programas de conscientização sobre a importância da proteção de dados pessoais para todos os cidadãos. De igual forma, é necessário um treinamento sobre gestão de dados, para capacitar aqueles que trabalham com alguma operação envolvendo dados pessoais.

Em caso de parceria público-privada de implantação de *smart city*, caberá às partes estabelecer, de forma expressa e clara, quem será o controlador dos dados pessoais e os limites de atuação do operador. De igual forma, importa determinar, por escrito, entre outras regras: a finalidade do tratamento; as responsabilidades de cada um quanto à segurança dos dados pessoais; as hipóteses de compartilhamento dos dados pessoais e quais os órgãos, instituições privadas e entidades públicas que terão acesso aos dados pessoais.

Por fim, entende-se importante a criação de uma estrutura de encarregados para o município, por ser uma entidade complexa com vários órgãos envolvidos com operações de tratamento de dados pessoais. O duplo DPO, conceito trazido pelo projeto europeu *SynchroniCity* [277] e estudado no próximo capítulo, é uma opção para a organização estrutural de entidades de grande porte, com uma estrutura complexa e que tratam grandes volumes de dados.

---

[276] WYLIE, Bianca. **Civic Tech: A list of questions we'd like Sidewalk plan for ist Toronto Project**. 30/10/2017. Torontoist. Disponível em: https://torontoist.com/2017/10/civic-tech-list-questions-wed-like-sidewalk-labs-answer/

[277] EUROPEAN COMMISSION**. SynchroniCity. Delivering na IoT enabled Digital Single Marketfor Europe and Beyond.** Disponível em: https://cordis.europa.eu/project/id/732240

2.5. Hipóteses de tratamento (bases legais) em cidades inteligentes

Neste tópico, optou-se por focar no sistema de proteção de dados pessoais brasileiro. Verifica questões de adequação de bases legais aos diversos tipos de tratamento de dados pessoais que ocorrem em tecnologias de *smart city*, utilizando alguns casos do exterior no contexto urbano nacional e exemplos hipotéticos.

Especificamente, estuda peculiaridades de bases legais de tratamento de dados pessoais nos âmbitos público e privado. Identifica quais bases legais são mais adequadas para cada setor na implantação de tecnologia em ambientes urbanos.

Uma das principais decisões a ser tomada pelo controlador antes de realizar o tratamento de dados pessoais é identificar a base legal aplicável ao seu tratamento. O processamento dos dados pessoais apenas será lícito se ele for enquadrado em, pelo menos, uma das situações previstas na legislação local.

É perfeitamente possível que a mesma operação de tratamento de dados pessoais possa ter fundamento em duas ou mais bases legais. Todavia, não se trata essa decisão apenas de uma escolha livre do controlador, pois, o que define qual a base legal a ser utilizada é a finalidade do tratamento[278].

Portanto, quando uma operação de tratamento é amparada em duas bases legais como, o consentimento e o legítimo interesse, e o titular dos dados revoga o seu consentimento, é possível continuar com o tratamento dos dados. No entanto, a licitude do tratamento dependerá da sua compatibilidade com a finalidade original.

No Brasil, o tratamento de dados pessoais deve ter uma base legal firmada em algum dos incisos do artigo 7º da LGPD ou, em caso de dados pessoais sensíveis, nos dispositivos constantes do artigo 11º. Desse modo, é necessário analisar caso a caso para saber qual das hipóteses de tratamento de dados pessoais seria mais adequada para cada situação.

Já quando o tratamento é realizado pelo Poder Público, também devem ser observadas as regras constantes no capítulo IV da LGPD, das quais envolve uma série de particularidades. Geralmente, elas decorrem da necessidade de harmonizar os exercícios de prerrogativas típicas do Estado com o regramento da LGPD[279].

---

[278] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** Abril de 2021. Disponível em: https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller 28-29 p.

[279] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 5 p.

Sabendo das peculiaridades do Poder Público, em junho de 2023, a ANPD publicou um guia orientativo para tratamento de dados pessoais neste setor. A intenção da entidade é de estabelecer parâmetros objetivos e segurança jurídica para as operações com dados pessoais realizadas por organizações públicas.

A ANPD analisou apenas algumas hipóteses de tratamento, quais sejam, o consentimento, o legítimo interesse, o cumprimento de obrigação legal e regulatória e a execução de políticas públicas[280]. O critério utilizado pela ANPD de escolha das hipóteses de tratamento para análise foi pelas bases legais mais comuns.

Apesar de o consentimento ter sido analisado pela ANPD neste material específico para o Poder Público[281], esta base legal não é a mais indicada para o tratamento de dados pessoais neste setor. Além do conhecimento exato sobre a finalidade do tratamento pelo titular, o consentimento dá ao titular dos dados o poder de recusar o tratamento ou revogar o seu consentimento, dado anteriormente, a qualquer momento.

Portanto, caso o poder público utilize a base legal do consentimento, é necessário que ele ofereça meios que assegurem o exercício do direito do titular de autorizar ou não o tratamento, bem como o revogar. Ainda, o consentimento deve ser concedido de forma que demonstre claramente a manifestação de vontade do titular.

O consentimento deve ter forma específica e destacada quando é a base legal escolhida para tratar de dados sensíveis. Aqui, a lei exige maior atuação do titular dos dados e um cuidado extra com o tratamento de dados do agente, uma vez que essa classe de dados propicia riscos significativos para o titular[282].

Um exemplo seria o consentimento de um paciente para conceder seus dados de saúde, estes considerados sensíveis, para um hospital público brasileiro. Adicione-se a esse exemplo a hipótese deste hospital participar de um sistema de compartilhamento de dados com outros controladores, como, hospitais, centros de saúde e de pesquisa, semelhante ao *The European Institute for Innovation through Health Data (*I~HD*).*

---

[280] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 10 p.

[281] Art. 5º inciso XII "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;" Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais**.

[282] TEPEDINO, Gustavo; FRASÃO, Ana; Oliva, Milena Donato e outros. **Lei Geral de Proteção de Dados Pessoais e as suas repercussões no Direito Brasileiro**. Revista dos Tribunais. Thomson Reuters. 2019. São Paulo. 341- 342 p.

Neste caso, o paciente deve consentir de forma específica, destacada e para determinada finalidade. A noção de consentimento específico e destacado está próxima de um consentimento expresso[283].

Interessante destacar a iniciativa do I~HD para envolver e capacitar os pacientes sobre assuntos relativos ao tratamento dos dados pessoais. Isso ocorre através da realização de programas de conscientização sobre os benefícios do compartilhamento e as medidas de segurança para proteger a privacidade. Além disso, o I~HD inclui representantes dos pacientes na sua equipe. [284]

O consentimento também é tido como uma das principais bases legais para o mercado privado. A adoção pela LGPD de um consentimento inequívoco como regra geral viabiliza o tratamento de dados na internet.[285]

Igualmente, o consentimento não deve ser a primeira opção de escolha do agente inserido no mercado privado, especialmente quando envolver dados pessoais com um potencial danoso significativo para o titular. Na maioria dos países, incluindo o Brasil, não há uma cultura em ler os pedidos de consentimento, o que acarreta em maior risco ao titular quando há uma real necessidade de envolvê-lo no tratamento.

A opção pelo consentimento ainda é menos indicada quando envolve dados pessoais sensíveis. A exemplo do TikTok, que foi multado em 12,700,000 euros por uma série de violações a UK GDPR, como a utilização ilegal de dados pessoais de crianças. O ICO alegou que o TikTok, além de não ter obtido o consentimento dos pais ou dos responsáveis pelos menores de 13 anos, não adotou medidas para identificar e remover crianças menores de idade na sua plataforma[286].

Outra base legal analisada pela ANPD para o Poder Público é o legítimo interesse, seja do controlador ou de terceiros, pelo tratamento de dados pessoais. Isso significa que o controlador pode aplicar essa base legal se valendo do interesse de outrem, que pode ser pessoa

---

[283] TEPEDINO, Gustavo; FRASÃO, Ana; Oliva, Milena Donato e outros. **Lei Geral de Proteção de Dados Pessoais e as suas repercussões no Direito Brasileiro**. Revista dos Tribunais. Thomson Reuters. 2019. São Paulo. 341 - 342 p.

[284] HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for Quality.** Disponível em https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality 2 p.

[285]LEONARDI, Marcel. **Principais bases legais para o tratamento de dados pessoais no setor privado**. Caderno especial LGPD. 2019. Editora RT. São Paulo. 75 p.

[286] IINFORMATION COMISSIONER'S OFFICE. *ICO Fines TikTok £12.7* **million for misusing children's data.** 04/04/2023. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/

natural ou jurídica, de direito público ou privado que não se enquadra nas categorias de controlador, operador ou encarregado[287].

Os possíveis interesses legítimos podem ter natureza negocial ou advirem da própria sociedade, através de interesse de uma categoria ou de toda a população. Alguns exemplos de uso do legítimo interesse de terceiros são a prevenção de fraude e a resposta a incidentes de segurança[288].

Esta autorização legal não se aplica em situações que prevalecem os direitos e liberdades fundamentais do titular, a exemplo de casos de tratamento de dados pessoais sensíveis[289]. Entende-se que essa decisão foi acertada, uma vez que tais informações não devem ser exploradas para fim comercial.

Como exemplo cita os dados pessoais de saúde, que requerem uma proteção especial devido ao maior risco relacionado ao seu uso, devido a sua capacidade de causar maior dano ao titular dos dados. Pelo fato de o dado de saúde ser considerado sensível, o legítimo interesse não pode ser aplicado e, portanto, o agente de tratamento terá que obter o consentimento específico e destacado do titular dos dados ou encontrar outra forma de enquadrar o tratamento em uma das alternativas previstas na LGPD[290].

Dada a sua flexibilidade, a adoção do legítimo interesse exige uma avaliação prévia capaz de demonstrar a proporcionalidade entre os interesses do agente e os direitos e as expectativas do titular de dados. Ainda, deve ser considerado que o titular dos dados pode exercer o seu direito de oposição, caso o tratamento descumpra algum dos requisitos previstos pela LGPD. A ANPD também não recomenda esta base de tratamento para o Poder Público [291]

A depender do caso, o legítimo interesse pode ser uma opção para o agente de tratamento do mercado privado, mesmo detendo o risco jurídico de documentar o relatório de impacto de proteção de dados pessoais que pode ser revisado e rejeitado pela ANPD[292]. Isto porque o RIPD

---

[287] JOELSONS, Marcela. **Lei Geral de Proteção de Dados. Fronteiras do Legítimo Interesse**. Indaiatuba, SP. Editora Foco. 2022. Edição do Kindle. 108 p.
[288] JOELSONS, Marcela. **Lei Geral de Proteção de Dados. Fronteiras do Legítimo Interesse**. Indaiatuba, SP. Editora Foco. 2022. Edição do Kindle. 109 p.
[289] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. 13 p.
[290] BRASIL. Autoridade Nacional de Proteção de Dados. **Estudo preliminar. Hipóteses legais de tratamento de dados pessoais: Legítimo interesse.** Versão 1.0. 4 p.
[291] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 13 p.
[292]LEONARDI, Marcel. **Principais bases legais para o tratamento de dados pessoais no setor privado.** Caderno especial LGPD. 2019. Editora RT. São Paulo. 78- 79 p.

já é uma exigência de implantação da *smart city*, independente de qual base legal será utilizada pelo agente.

Um exemplo interessante para análise é a possível aplicação da base legal do legítimo interesse para tecnologia relacionada a segurança, como a instalação de câmeras de vigilância em um shopping. De acordo com a ANPD, o shopping pode utilizar essa base legal para tratar dados de câmeras de segurança em suas dependências[293].

A ANPD entende que o shopping pode tratar, inclusive dados pessoais de crianças e adolescentes, porque o princípio do melhor interesse do menor é compatível com o tratamento. A segurança do menor será zelada, além de potencializar as chances de encontra-lo, caso ele se perca.

No entanto, o shopping deve adotar medidas de mitigação de risco, tais como um prazo curto de armazenamento dos dados e a não utilização de tecnologias que tratem as imagens de forma biométrica. Além disso, deve observar o princípio da necessidade na realização do planejamento da segurança, com o propósito de reduzir o número de câmeras a serem instaladas no estabelecimento.

Ademais, será necessário que o shopping elabore um relatório de impacto à proteção dos dados pessoais, uma vez que este tratamento pode causar um grande prejuízo aos dados pessoais, às liberdades civis e aos direitos fundamentais dos cidadãos.

No entanto, se utilizasse a base legal do interesse legítimo para o caso do Smart Sampa[*294*], programa de videomonitoramento de segurança pública, haveria problemas com o entendimento da ANPD, pois, o Smart Sampa determina um alto número de câmeras instaladas pela cidade – quarenta mil no total – e o uso de biometria facial. Ainda, pelo fato de o controlador ser uma entidade pública, há bases legais mais adequadas para este tipo de tratamento, como a execução de políticas públicas.

Uma vez escolhido o legítimo interesse como base legal de tratamento, o agente, público ou privado, deve realizar um teste com três etapas: finalidade, que irá identificar se o interesse é próprio ou de terceiros; necessidade, verifica a obrigatoriedade de realizar o tratamento para

---

[293]BRASIL. Autoridade Nacional de Proteção de Dados. **Estudo preliminar. Hipóteses legais de tratamento de dados pessoais: Legítimo interesse.** Versão 1.0.. 9 p.

[294] PREFEITURA DE SÃO PAULO. **Prefeito assina contrato para o início do Smar tampa, maior programa de videomonitoramento da cidade com até 40 mil câmeras**. Cidade de São Paulo. 07/08/2023. Disponível em*:* https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2

alcançar o objetivo e; proporcionalidade, averigua o equilíbrio entre o interesse legítimo e os direitos e as liberdades fundamentais do titular[295].

O cumprimento de obrigação legal ou regulatória também é uma base legal de tratamento estudada pela ANPD para o Poder Público. Essa hipótese de tratamento se aplica, como regra geral, em dois assuntos normativos distintos, quais sejam, sob as normas de conduta e as regras de organização do Poder Público[296].

A norma de conduta é uma regra de comportamento imposta pela lei e, caso não seja cumprida pelo Poder Público, pode ser objeto de penalidade administrativa. Neste contexto, é necessário o tratamento de dados pessoais para acatar uma imposição normativa de uma obrigação legal expressa ou de uma determinação regulatória constituída por um órgão regulador. O controlador que adere a esta hipótese de tratamento deve informa-la ao titular dos dados.

Quando o cumprimento de obrigação legal ou regulatória é inerente a uma norma de organização, ele tem como objetivo estruturar órgãos e entidades públicas, estabelecendo suas competências e atribuições. Desse modo, o tratamento de dados pessoais é parte essencial ao cumprimento de atribuições legais típicas daquela entidade ou órgão, ou seja, é necessário para viabilizar a execução, a competência e a finalidade pública daquele ente administrativo.

Neste sentido, vale mencionar o projeto de lei de nº 976/21, o qual fomenta a política de desenvolvimento das cidades inteligentes no Brasil. A sua redação estabelece que o uso de dados pela Administração Pública em projetos de cidades inteligentes deve observar as restrições e o ordenamento da LGPD[297].

Ainda, o relatório do projeto destaca a criação, pela União, de cláusulas específicas para o uso de tecnologia TIC, especialmente, para casos de uso de ferramentas tecnológicas que

---

[295] LEONARDI, Marcel. **Principais bases legais para o tratamento de dados pessoais no setor privado.** Caderno especial LGPD. 2019. Editora RT. São Paulo. 79 p.

[296] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. 15 p.

[297] "Com relação aos aspectos do uso de dados, em primeiro lugar, é importante ressaltar que esse tipo de iniciativa deve se inserir em um contexto maior e específico ditado pela LGPD – Lei Geral de Proteção de, instituída pela Lei no 13.709, de 2018. Assim, o uso de dados pela Administração em projetos de cidades inteligentes deve observar as restrições e o ordenamento contido na LGPD, em especial a observância da privacidade e da segurança das informações, assim como o uso das melhores práticas. A integração dos serviços e o compartilhamento de dados entre entes da Administração deverão seguir estritamente as regras lá contidas que estabelecem, entre outros ditames, que o tratamento deve se dar para a execução de políticas públicas específicas e aprovadas. Da mesma forma, os dados coletados não podem objetivar sua comercialização de forma identificada. Todos esses cuidados devem continuar a serem seguidos". BRASIL. Câmara dos Deputados. PL 976/2021. **Política Nacional de Cidades Inteligentes.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2274449 19 p.

necessitarão de um padrão de interoperabilidade, condições e direito de uso e reuso dos dados. Nestas hipóteses, o objetivo do tratamento é fomentar a inovação de soluções ou de serviços[298].

Um exemplo hipotético seria a implantação, por imposição legislativa, de um sistema digital de governança de dados sob aplicativos de mobilidade urbana, que exigiria, para o seu funcionamento, o cadastro dos seus usuários. Assim, a proteção dos dados pessoais dos titulares, inerente a prestação do serviço de mobilidade urbana pública, seria imposta pela referida lei, sob as regras da LGPD.

No exemplo acima, o tratamento dos dados pessoais pelo Poder Público é legítimo, já que está diretamente vinculado ao cumprimento de norma de conduta através de uma obrigação legal definida por lei específica, nos termos do artigo 7º inciso II da LGPD.

Outro exemplo é a criação de um sistema, que utiliza IA e *big data*, por uma agência reguladora, para tratar dados pessoais dos seus servidores com a finalidade específica de realizar os pagamentos de salários e benefícios previdenciários. Esta obrigação estaria expressamente prevista em uma legislação específica e, portanto, o tratamento de dados pessoais se fundamentaria sob a base de cumprimento de obrigação legal.

Para o mercado privado, também é possível existir uma legislação específica, que impõe uma obrigação legal ou regulatória ao controlador, relativo a uma operação de dados pessoais. Portanto, é de suma importância que o agente de tratamento conheça os regulamentos específicos do seu setor de atuação, tais como as áreas financeira e de saúde suplementar.

Nestas hipóteses, a natureza das normas, por si só, justifica a adoção da base legal do cumprimento de obrigação legal ou regulatória. Cumpre ressaltar que este tratamento é limitado à finalidade específica e, portanto, caso o agente opte por realizar o tratamento desses dados pessoais para outra finalidade, será necessário que ele recorra a outra base legal que justifique o novo tratamento.

Um exemplo dessa situação é a resolução BCB nº 85 de 08/04/2021 do Banco Central, que contém normas relativas à política de segurança cibernética, plano de ação e de respostas a incidentes, contratação de serviços de processamento e armazenamento de dados em computação em nuvem, direcionadas às instituições financeiras na implantação do PIX[299]. Para

[298]BRASIL. Câmara dos Deputado. **PL 976/2021.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2274449. 19 – 20 p.

[299] BANCO CENTRAL DO BRASIL. **Resolução BCB nº 85 de 08/04/2021**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85

executar diversas normas da referida resolução, devem-se realizar vários tratamentos de dados pessoais.

No entanto, caso a instituição financeira resolva tratar os mesmos dados pessoais para uma finalidade diversa da resolução, como, por exemplo, para fim comercial, então a entidade deverá escolher outra base legal para este tratamento.

A última base legal tratada pela ANPD para o Poder Público é a execução de políticas públicas. O artigo 7º inciso III da LGPD determina o tratamento ou o uso compartilhado de dados que seja necessário à execução de políticas públicas que estejam previstas em leis, regulamentos, contratos, convênios ou instrumentos congêneres.

Para esta análise, a ANPD considerou o termo "administração pública" como sinônimo de Poder Público, e, portanto, abrange as entidades e os órgãos dos poderes executivo, legislativo e judiciário. Quanto ao termo "políticas públicas", não definido pela LGPD, a ANPD entendeu que pode ocorrer por, pelo menos, dois meios, ou através de atos normativos ou por ajustes contratuais[300].

Em caso de tratamento de dados sensíveis baseado em políticas públicas, o entendimento da ANPD foi pela adoção restrita, considerando apenas a autorização dessa base legal através de leis ou regulamentos. O argumento da entidade foi que o artigo 11, inciso I, b, da LGPD não faz referência às políticas públicas advindas de ajustes contratuais.

Já a definição material de políticas públicas consiste em um programa ou ação governamental específica, executada por entidade ou órgão público. A ANPD adotou um conceito amplo, que abrange todo e qualquer programa ou ação governamental definido em instrumento formal, com objetivos, meta, prazo e meios de execução. Por fim, esta hipótese também deve observar o artigo 23 da LGPD, especialmente quanto a exigência da finalidade pública do tratamento[301].

Um exemplo hipotético de utilização dessa base legal em implantação de *smart city* em cidades brasileiras seria a utilização de uma plataforma de dados, semelhante à *London Datastore,*[302]*,* para controlar o índice de tabagismo entre os cidadãos. Neste caso, a Secretaria

---

[300] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 20 p.

[301] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.**. Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf p.21

[302]MAYOR OF LONDON. **London Datastore.** Disponível em: https://data.london.gov.uk/?_gl=1%2a17r8k54%2a_ga%2aNDA4NzczMTUuMTY3ODg3NjIzNA..%2a_ga_PY4SWZN1RJ%2aMTY3OTM4OTEwMy4xLjAuMTY3OTM4OTEwMy42MC4wLjA.

de Saúde estadual usaria os dados pessoais para desenvolver políticas públicas de prevenção ao câncer de pulmão.

Nesta hipótese, haveria uma legislação estadual prévia, que regularia o tratamento de dados pessoais realizado pela Secretaria de Saúde do estado. Por conta dos dados sensíveis relacionados a saúde do cidadão, o tratamento seria realizado com base no artigo 11, inciso II, b da LGPD[303].

Para o mercado privado, é válido mencionar duas hipóteses legais de tratamento que são a execução de contrato ou de procedimentos preliminares que se relacionam com o contrato do qual o titular faz parte e a proteção de crédito. O primeiro admite o tratamento de dados pessoais na cadeia de serviços e produtos contratados pelo titular dos dados, caso o tratamento seja necessário para o cumprimento do contrato ou para a realização de procedimentos preliminares relacionados[304].

Como exemplo hipotético de aplicação dessa base legal, suponha-se uma compra de um determinado vestuário personalizado, através de um site, que compartilharia os dados pessoais do cliente com o fabricante e com o distribuidor. O cliente tem um contrato principal com o fornecedor intermediário e este possui dois contratos em sua cadeia de fornecimento do produto, um com o fabricante do item e o outro com a distribuidora.

Assim, para cumprir com o acordo principal, é preciso compartilhar os dados pessoais do cliente como, as suas características físicas, a exemplo das medidas do seu corpo, e o seu endereço residencial. Desse modo, cada uma das empresas irá realizar o tratamento de dados pessoais, podendo utilizar a execução do contrato como base legal de cada tratamento.

Por fim, a LGPD inova ao definir a proteção de crédito como base legal autônoma de tratamento de dados pessoais. Todavia, a lei não traz o significado de proteção de crédito, cabendo à ANPD optar ou por um conceito restritivo, considerando apenas as atividades inerentes a proteção de crédito, ou por uma definição abrangente, que também inclui a este conceito as atividades de apoio, como o oferecimento de produtos e serviços de crédito[305].

Esta opção de base legal é interessante para as instituições financeiras que podem realizar uma gestão do risco de crédito, seja na contratação de um financiamento ou na liberação de um cartão de crédito. Um exemplo dessa base legal seria a utilização de um software pela

---

[303] Art. 11, inciso II. "b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;" Lei nº 13.709/2018. **Lei Geral de Proteção de Dados Pessoais.**

[304] LEONARDI, Marcel. **Principais bases legais para o tratamento de dados pessoais no setor privado**. Caderno especial LGPD. 2019. Editora RT. São Paulo. 77-78 p.

[305] LEONARDI, Marcel**. Principais bases legais para o tratamento de dados pessoais no setor privado**. Caderno especial LGPD. 2019. Editora RT. São Paulo. 84 p.

instituição financeira para fixar um limite de crédito flexível, de forma automatizada e baseada no histórico do cliente[306].

Além do mais, essa opção também pode ser executada por estabelecimentos comerciais, como para maior segurança de recebimento do valor devido pela prestação de um serviço ou fornecimento de um produto. A partir dos dados do cidadão, como, CPF, endereço, renda e telefone, é realizada a pesquisa para identificar restrições cadastrais perante órgãos de proteção de crédito.

Neste sentido, o credor não precisa do consentimento do devedor para o tratamento dos dados pessoais, até para inclui-lo nos cadastros, podendo fazê-lo pela hipótese da proteção do crédito. Todavia, conforme o CDC[307], é preciso observar os direitos do consumidor como o seu direito de verificar as suas informações, sejam em bancos de dados públicos ou privados, e de solicitar a retificação quando estiverem incorretas[308].

2.6. Compartilhamento indevido e desvio de finalidade

Este tópico investiga os desafios para evitar o compartilhamento indevido de dados pessoais e o desvio de finalidade no seu tratamento, especialmente no contexto de cidades inteligentes. O objetivo é detectar as práticas ilegais de compartilhamento e de uso indevido dos dados pessoais em situações que se relacionam com tecnologias *smart city* e que podem comprometer a proteção dos dados.

Também, analisa casos sobre dados pessoais armazenados em outros países relativos a cidadãos estrangeiros. Em cidades inteligentes, é comum haver tecnologias estrangeiras que coletam e transferem os dados pessoais dos cidadãos locais para outro país, criando o risco de acesso aos bancos de dados de empresas de tecnologia pelo governo estrangeiro.

Primeiramente, é preciso esclarecer a importância do compartilhamento legal de dados pessoais, especialmente para o funcionamento e para criação de uma série de serviços e produtos tecnológicos destinados à prestação do serviço público[309]. Os sistemas europeu e

---

[306] PARENTONI, Leonardo. **Compartilhamento dos dados e a figura do controlador.** 2021. Disponível em: https://www.researchgate.net/profile/Leonardo-Parentoni 28 p.

[307] Artigos 43 e seguintes da lei de número 8.078 de 11 de setembro de 1990. **Código de Defesa do Consumidor.**

[308] BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Banco de Dados e Cadastros dos Consumidores**. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/bancos-de-dados-e-cadastros-de-consumidores

[309] Inclusive, o Projeto de Lei 976.2021 adota o compartilhamento de dados, como diretriz da implantação de cidade inteligente no Brasil "Art. 5º O desenvolvimento de iniciativas de cidades inteligentes deverá observar as seguintes diretrizes: VI – compartilhamento de dados e informações entre entes federativos;" BRASIL. Câmara dos Deputados. Projeto de lei 976.2021**. Política Nacional de Cidades Inteligentes (PNCI)** disponível em: https://www.camara.leg.br/propostas-legislativas/2274449

brasileiro de proteção de dados pessoais possuem dispositivos que regulamentam o compartilhamento de dados pessoais, alguns verificados neste trabalho por meio dos casos concretos.

Sem o compartilhamento de dados pessoais entre dispositivos tecnológicos, a implantação de tecnologia no ambiente urbano e a inovação ficariam comprometidas em vários setores públicos, a exemplo da segurança, da saúde e da mobilidade urbana. Assim, é essencial identificar o que o sistema de proteção de dados pessoais local entende como compartilhamento lícito de dados, distingui-lo do compartilhamento ilícito e aprimorar os produtos e serviços de tecnologias TIC.

De início, destaca-se o uso secundário dos dados pessoais, que ocorre quando o dado começa a ser utilizado para a finalidade original, mas, em situação posterior, passa a ser utilizado para finalidade diversa. Esta nova utilização pode ser executada pelo mesmo agente de tratamento ou por iniciativa de outros sujeitos. [310]

O uso secundário é admitido pelos sistemas de proteção de dados pessoais, a exemplo do GDPR.[311] Todavia, caso ocorra o uso secundário sem a observância dos ditames impostos pelo referido diploma, essa prática será considerada ilícita e, portanto, sujeita a sanções.

O uso secundário de dados pessoais tem grande importância para o crescimento do mercado de dados, inclusive para as cidades inteligentes, pois permite que o ordenamento normativo de proteção de dados seja compatível com formas de circulação dos dados. Um

---

[310] "Um dos pontos centrais da pretendida compatibilização é o chamado uso secundário dos dados pessoais, que ocorre quando o dado originariamente coletado para determinada finalidade passa a ser posteriormente utilizado para finalidade diversa, por ordem do mesmo controlador ou até por inciativa de sujeitos diferentes. O GDPR expressamente admite o uso secundário." PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** 2021. Disponível em: https://www.researchgate.net/profile/Leonardo-Parentoni 21 p.

[311] Considerando (50) "The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations". EUROPEAN UNION. **European Parliament. Regulation nº 2016/679/CE.** Brussels. 27/04/2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

exemplo disso é a compatibilidade do ordenamento com o *big data,* tecnologia presente nos ambientes urbanos,[312] que armazena informações e as processam para diversas finalidades.

O compartilhamento de dados pessoais[313] é uma das formas de uso secundário de dados, e acontece quando o dado tratado por um controlador também é utilizado por outros agentes em outras operações de tratamento. Esta é uma das práticas mais importantes para o desenvolvimento de uma cidade inteligente. Através dela, os pesquisadores e desenvolvedores de tecnologia compartilham conhecimento entre si para potencializar a prestação de serviços públicos, criar produtos e oferecer novas oportunidades para outros mercados, aquecendo a economia.

Um exemplo de compartilhamento é o DTG 3.0 em Barcelona, tratado no item 1.2 deste trabalho, que objetiva criar uma plataforma a partir de dados coletados por sensores espalhados pela cidade e instalados em veículos. Várias organizações terão acesso a esse banco de dados, como fabricantes automobilísticos, prestadores de serviços e o governo local, cada um com a sua finalidade, além de compartilhar informações que serão úteis para o desenvolvimento do transporte público.

Outros exemplos são a *London Datastore,* plataforma aberta de dados públicos que compartilha dados com diversos fornecedores para aprimorar diferentes serviços e produtos, e a *European Institute for Innovation through Health Data*, que compartilha dados coletados em postos de saúde com órgãos de pesquisa para desenvolver novos medicamentos. Portanto, o Direito não pode coibir o compartilhamento, que é fundamental para os desenvolvimentos humano, econômico e urbano, mas criar meios de punição e de prevenção contra práticas de compartilhamento fora dos limites legais.

Um dos mais notórios casos de compartilhamento indiscriminado de dados é o do *TikTok*, aplicativo chinês de vídeos curtos. Suspeita-se que o *TikTok* compartilha dados dos seus usuários com o governo chinês, para fins comerciais e políticos.

Por conta da sua vasta gama de usuários de diferentes nacionalidades, este caso gerou uma discussão mundial sobre a proteção de dados pessoais e a privacidade. Em pesquisa

---

[312] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador**. 2021. Disponível em: https://www.researchgate.net/profile/Leonardo-Parentoni 26 p.

[313] "Dentro das várias possibilidades de uso secundários dos dados, uma das mais importantes (e polêmicas) é o compartilhamento, ou seja, quando o dado pessoal tratado por ordem de determinado controlador passa a ser utilizado também em operações de tratamento realizadas por terceiros, seja na condição de controladores ou de operadores." PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador.** 2021. Disponível em: https://www.researchgate.net/profile/Leonardo 23- 24 p.

realizada no ano de 2023, foi constatado que o aplicativo possui mais de 1 bilhão de usuários no mundo, sendo que, só nos EUA, são 116, 5 milhões de usuários e, no Brasil, 84,1 milhões[314].

O *TikTok* pode acessar uma série de dispositivos dos usuários como câmera, microfone, conexão de Wi-Fi, agenda de contatos, álbum de fotos, endereço IP da internet, localização do usuário e leitura e registro de dados no armazenamento do dispositivo[315]. A plataforma é controlada pela empresa *ByteDance,* sediada na China e regulada pela Lei de Inteligência Nacional chinesa.

Esta legislação impõe às empresas nacionais chinesas o compartilhamento de seus dados com as autoridades locais, quando solicitado[316]. A incerteza sobre a existência desse compartilhamento estremeceu as relações entre a *ByteDance* e os governos estrangeiros, sobretudo gerando proibições do uso do *TikTok* em alguns países[317].

Em março de 2023, o CEO do TikTok, Shou Zi Chew, foi interrogado por legisladores americanos. Apesar de Chew ter negado veementemente que o aplicativo compartilhasse dados dos seus usuários com o governo chines, houve um forte impulso legislativo para proibir a plataforma nos EUA[318].

No mesmo mês, o congresso americano deu início a tramitação do projeto de lei S.686 chamado *Restrict Act*, cujo objetivo é restringir o uso de aplicativos tecnológicos que são considerados uma ameaça à segurança nacional[319]. Todavia, apesar de ser conhecido popularmente como *TikTok bill*, este projeto de lei não se limita a esse aplicativo.

Houve ainda amplas ações do governo federal americano e de alguns governos estaduais para proibir o *TikTok* em dispositivos governamentais. O estado de Montana foi mais longe e baniu o *TikTok* das lojas de aplicativos móveis do estado[320].

---

[314]DATAREPORTAL. **TikTok users, stats, data & trends.** 11/05/2023 Disponível em: https://datareportal.com/essential-tiktok-stats

[315] TIKTOK. **Privacidade e segurança no TikTok.** Disponível em: https://www.tiktok.com/safety/pt-br/privacy-and-security-on-tiktok/

[316] ROSENVALD, Nelson; DIAS, Daniel; FORTES, Pedro; VENTURI, Thais G. Pascoaloto. **Plataformas digitais e a (in)segurança de dados: O cerco ao TikTok**. MIGALHAS. 24/04/2023. Disponível em: https://www.migalhas.com.br/coluna/direito-privado-no-common-law/385252/plataformas-digitais-e-a-in-seguranca-de-dados-o-cerco-ao-tiktok

[317]EURONEWS. **Quais países que proibiram o TikTok e porquê?** 27/03/2023 Disponível em: https://pt.euronews.com/next/2023/03/27/quais-os-paises-que-proibiram-o-tiktok-e-porque

[318] SHEPARDSON, David; AYYUB, Rami. **TikTok congressional hearing: CEO Shou Zi Chew grilled by US lawmakers.** REUTERS. 24/03/2023. Disponível em: https://www.reuters.com/technology/tiktok-ceo-face-tough-questions-support-us-ban-grows-2023-03-23/

[319]CONGRESS.GOV. **S.686- RESTRICT Act**. 2023. Disponível em:. https://www.congress.gov/bill/118th-congress/senate-bill/686?s=1&r=15

[320] JONNAVITHULA, Ani; SAYED, Pantho. **The TikTok Bill Isn't Only About TikTok**. Jolt Digest. 26/04/2023. Disponível em: https://jolt.law.harvard.edu/digest/the-tiktok-bill-isnt-only-about-tiktok

Nada impede que o caso *TikTok* ocorra com tecnologias *smart city* inseridas em ambientes urbanos, especialmente com o endurecimento de normas sobre a segurança e o compartilhamento dos dados. Agora, a atenção das empresas de TIC com normas relativas aos dados pessoais vai para além da prevenção de punições menos gravosas como advertências e multas pecuniárias, mas para evitar o banimento de seus produtos e serviços em grandes mercados.

Outro episódio importante para este estudo é o da META, empresa americana de tecnologia e mídia social. Em 2023, a META foi multada pelo *Data Protetction Comissioner* (DPC) em 1,3 bilhão de dólares por violar o GDPR através de tratamento indevido de informações dos seus usuários, especialmente pela transferência não autorizada de dados pessoais entre a empresa localizada na União Europeia e seus servidores nos Estados Unidos[321]

O fato gerador da punição foi a utilização de dados dos usuários para encaminhar anúncios baseados em seus comportamentos. Esta ação ocorreu na Irlanda e foi executada pela Meta Ireland.

Este caso escancara a diferença legislativa entre os sistemas de proteção de dados da União Europeia e dos Estados Unidos, especialmente porque este permite que as agências de inteligência americanas interceptem comunicações no exterior, inclusive correspondência digital. [322]

Foi considerado pelo Tribunal de Justiça da UE a existência de risco de acesso aos dados pessoais dos usuários europeus da META por autoridades americanas. Ainda, a decisão sustentou que a legislação dos EUA não fornece um nível de proteção de dados equivalente ao exigido pela UE e que a META não executou medidas suplementares de proteção dos dados pessoais para compensar as legislações dos EUA, não adequando o seu nível de proteção conforme regras da UE[323].

A META alegou que a transferência de dados é fundamental para operar e fornecer os seus serviços. Ademais, sem a capacidade de transferir dados entre países, o funcionamento da internet aberta global estaria comprometido.

---

[321]HALPIN, Padraic. **Meta hit with record $1.3 bln fine over data transfers** REUTERS. 22/05/2023. Disponível em: https://www.reuters.com/technology/facebook-given-record-13-bln-fine-given-5-months-stop-eu-us-data-flows-2023-05-22/

[322]ROSENVALD, Nelson; DIAS, Daniel; FORTES, Pedro; VENTURI, Thais G. Pascoaloto A **A histórica multa aplicada pela União Europeia à META pelo compartilhamento não autorizado de dados de seus usuários com os EUA.** MIGALHAS. 30/05/2023. Disponível em: https://www.migalhas.com.br/coluna/direito-privado-no-common-law/387351/a-historica-multa-aplicada-pela-uniao-europeia-a-meta

[323] EUROPEAN DATA PROTECTION BOARDING. **Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation.** Disponível em: https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en 67- 68 p.

Depois de algumas negativas, por parte da União Europeia, sobre tentativas de acordo de transferência de dados, em julho de 2023 a UE anunciou um novo pacto de transferência de dados pessoais com os EUA. Este acordo se concretiza três anos depois do Tribunal de Justiça da UE ter invalidado a decisão de adequação anteriormente estabelecida (Acordão Schrems II).[324]

Esta decisão representa um marco na proteção de dados, uma vez que o modelo de livre circulação voltado apenas para atender aos interesses de empresas privadas já não é mais admitido[325]. Agora, todas as empresas que tratam dados pessoais, inclusive aquelas de tecnologia *smart city*, precisam estar atentas às políticas governamentais de proteção de dados, sob pena de sofrer graves punições.

Um exemplo é a criação do *Standard Contractual Clauses* (SCC) pela União Europeia, que são cláusulas contratuais padrão que tem como finalidade garantir medidas adequadas de proteção de dados pessoas impostas a entidade estrangeira amparada por legislação incompatível com a UE. Em 2021, a Comissão Europeia modernizou o SCC conforme o GDPR, para a transferência de dados de agentes de tratamento de dentro da UE para agentes de tratamento localizado em outros países[326]

Algumas das novidades da SCC de 2021 são a inclusão de obrigações estabelecidas pelos novos requisitos do GDPR, como a imposição da transparência, da confecção de cláusulas mais detalhadas sobre os direitos dos titulares de dados pessoais e da notificação de violação dos dados. Além do mais, as partes que aderirem o SCC devem realizar o "*transfer impact assessment*"[327].

Em 2020, no Brasil, a Presidência da República editou a medida provisória nº 954, que previa o compartilhamento de dados pessoais de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Pesquisa – IBGE. A finalidade do compartilhamento era produzir estatísticas de distanciamento social para o combate à pandemia COVID 19.

---

[324] EURONEWS. **UE dá luz verde para partilha de dados pessoais com os EUA.** 10/07/2023. Disponível em: https://pt.euronews.com/my-europe/2023/07/10/ue-da-luz-verde-para-partilha-de-dados-pessoais-com-os-eua.

[325] ROSENVALD, Nelson; DIAS, Daniel; FORTES, Pedro; VENTURI, Thais G. Pascoaloto A **A histórica multa aplicada pela União Europeia à META pelo compartilhamento não autorizado de dados de seus usuários com os EUA**. MIGALHAS. 30/05/2023. Disponível em: https://www.migalhas.com.br/coluna/direito-privado-no-common-law/387351/a-historica-multa-aplicada-pela-uniao-europeia-a-meta 3

[326]EUROPEAN COMMISSION. **Standard Contractual Clauses (SCC)** 04/06/2021. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[327] EUROPEAN COMMISSION. **New Standard Contractual Clauses – Questions and Answers overview.** Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en Acesso em 30/11/2023.

Foram propostas cinco ações diretas de inconstitucionalidade (ADI) contra a MP 954. O STF deferiu as medidas cautelares das ADIs, considerando inconstitucional o compartilhamento de dados previsto na MP 954, por violação dos direitos à intimidade, à vida privada e ao sigilo de dados.

Algumas das alegações dos ministros do STF que votaram contra a MP foram: o desrespeito aos princípios da razoabilidade e da proporcionalidade na relativização dos direitos e garantias fundamentais e que o compartilhamento de dados para tal finalidade deveria preceder de debate público sobre a necessidade, a relevância e a urgência da medida.[328]

A finalidade de coleta de dados pessoais da MP era legítima, mas os meios pelos quais houve o tratamento não foram claros e, por conta disso, a MP violou os princípios da transparência, da finalidade e da necessidade[329]. Ressalta que esse julgamento foi um marco para a proteção dos dados pessoais no Brasil porque, pela primeira vez, o STF definiu a proteção dos dados pessoais como um direito fundamental autônomo e, na época, implícito na CF/88.

Entende-se que este precedente jurisprudencial também é importante na implantação de tecnologia *smart city* em ambiente urbano que utiliza dados pessoais. Esta decisão evidencia a necessidade da participação popular nos projetos de inserção das tecnologias em espaços públicos que colocam em risco direitos e garantias fundamentais dos cidadãos.

Os debates públicos são fundamentais para proporcionar a todos uma voz ativa em situações de interesse coletivo. No caso específico de s*mart city,* devem ser ouvidos, tanto os desenvolvedores de tecnologias TIC como os juristas especializados na área, sobre as limitações tecnológicas em garantir a proteção dos dados pessoais e dos direitos fundamentais, conforme estudado em tópicos anteriores.

É igualmente importante a participação de grupos menos favorecidos, como representantes de pessoas com deficiência e de idosos, para verificar as melhores condições tecnológicas de inclusão social destes grupos. Por fim, os debates públicos servem para esclarecer dúvidas e mostrar os gastos relativos às implantações tecnológicas.

Ainda em 2020, foram ajuizadas ADI e ADPF contra o decreto de nº 10.046/2019, da Presidência da República, do qual dispõe sobre a governança e o compartilhamento de dados. Um dos argumentos dos proponentes é que a referida MP geraria uma espécie de vigilância em massa.

---

[328]BRASIL. Supremo Tribunal Federal . STF **suspende compartilhamento de dados de usuários de telefonias com IBGE.** 07/05/2020. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1

[329] PARENTONI, Leonardo Netto. **Compartilhamento dos dados e a figura do controlador**. 2021. Disponível em: https://www.researchgate.net/profile/Leonardo-Parentoni 29-30 p.

Em 2022, por maioria de votos, o STF decidiu que órgãos e entidades da administração pública federal podem compartilhar dados pessoais entre si, mas devem observar alguns critérios. Um deles é a justificativa formal, prévia e detalhada sobre a necessidade de inclusão de novos dados pessoais na base integradora[330].

Para o STF, a administração pública deve compartilhar o mínimo de dados necessário para atender à finalidade pretendida e informada. As entidades públicas controladoras também devem atender a todas as exigências da LGPD, cumprindo seus requisitos, garantias e procedimentos.

O Supremo também impôs ao Comitê Central de Governança de Dados a criação de medidas de segurança em conformidade com a LGPD, especialmente para o sistema eletrônico de registro de acesso. Também foi decidido pela limitação do compartilhamento de informações pessoais com agências de inteligência, que só pode ocorrer por meio de legislação específica, interesse público e parâmetros fixados pelo julgamento da ADI 6529[331].

Este julgado também tem a sua importância para a implantação de *smart city* no ambiente urbano. O compartilhamento indevido de dados pessoais entre organizações, sejam elas públicas ou privadas, pode acarretar em uma série de violações aos direitos e garantias do cidadão, a exemplo do monitoramento excessivo, a ser estudado em tópico posterior.

Porém, em muitos casos é necessário o compartilhamento de dados para a maior eficiência na prestação de serviços públicos, a inovação e a desburocratização estatal. Inclusive, em algumas hipóteses, é preciso tratar os dados para uma finalidade diversa da original, caso seja compatível com o interesse público[332].

Como já foi verificado, a tecnologia *smart city* implantada para potencializar serviços públicos necessita, em várias ocasiões, de compartilhar os dados pessoais. Da mesma forma que na Europa, o compartilhamento de dados pessoais no Brasil também deve observar uma série de requisitos, de acordo com o caso concreto.

As principais prerrogativas para o compartilhamento de dados pessoais no Brasil foram analisadas pela ANPD e decorrem da própria LGPD. Estes e outros requisitos devem ser

---

[330] BRASIL. Supremo Tribunal Federal. **STF valida compartilhamento de dados mediante requisitos. O Plenário também fixou restrições à atuação do Comitê Central de Governança de Dados**. 20/10/2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1

[331] Trata-se de julgamento acerca de ADI contra norma de competência da Presidência da República sobre a defesa das instituições e dos interesses nacionais, que estaria condicionada ao fornecimento de dados e conhecimentos específicos para a Agência de Inteligência Brasileira (Abin). BRASIL. Supremo Tribunal Federal . **Partidos questionam norma que condiciona fornecimento de dados à Abin a ato presidencial.** Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449429&ori=1

[332] PARENTONI, Leonardo. **Compartilhamento dos dados e a figura do controlador.** 2021. Disponível em: https://www.researchgate.net/profile/Leonardo-Parentoni 34 p.

observados, especialmente quando a implantação da tecnologia *smart city* ocorrer com a participação do Poder Público.

Por conseguinte, são requisitos para o compartilhamento de dados do Poder Público: a formalização e o registro do compartilhamento; a indicação dos dados pessoais que serão compartilhados e a sua finalidade, que deve ser específica; a indicação da base legal utilizada; a delimitação do período de duração do uso compartilhado dos dados; o acesso facilitado de informações claras e precisas sobre o compartilhamento e o direito dos titulares e; as medidas de segurança adotadas para proteger os dados pessoais[333].

2.7. Incidentes de segurança

Este item verifica relatórios de incidentes de segurança, com o propósito de entender o seu grau de ocorrência. Identifica casos concretos de incidentes de segurança com dados pessoais, ocorridos em setores públicos e em mercados privados, no Brasil e no estrangeiro.

Ainda, descreve as medidas das Autoridades de Proteção de Dados quando identificadas ações contrárias aos padrões de segurança exigidos pela legislação. Por fim, estuda quais os riscos de ocorrência dos incidentes de segurança em cidades inteligentes.

Um incidente de segurança com dados pessoais é qualquer evento que tem como resultado a destruição, perda, alteração ou o vazamento desses dados. Esta violação pode ocorrer através do acesso não autorizado, acidental ou ilícito ou por meio de um tratamento de dados ilícito ou inadequado, que cria riscos para os direitos e liberdades do titular dos dados pessoais[334].

O aumento do uso da internet e de dados foi seguido por um crescimento de ameaças cibernéticas e vazamento de dados. No entanto, as regulações e os padrões de segurança não conseguiram evitar uma parte significativa desses incidentes.

Em um relatório sobre incidentes de segurança publicado em 2021, indica um número expressivo de ataques cibernéticos ocorridos no mundo todo, no ano de 2020, contra empresas

---

[333] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. Junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf 29 p. e seguintes

[334] BRASIL. Autoridade Nacional de Proteção de Dados Pessoais **Incidentes de segurança com dados pessoais**. Ministério da Justiça e Segurança Pública. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais#:~:text=Um%20incidente%20de%20seguran%C3%A7a%20com,dados%20inadequada%20ou%20il%C3%ADcita%2C%20os

privadas e órgãos governamentais que atuam em diferentes setores[335]. Isso mostra que nenhum controlador está isento de sofrer um incidente de segurança.

Figura 3. Gráficos do relatório sobre incidentes de segurança da *Kaspersky.* [336]

O primeiro gráfico da figura 3 detalha a ocorrência dos incidentes de segurança em cada continente. Destaque para a alta incidência de *ransomware*[337] nas Américas.

Já o segundo gráfico da figura 3 identifica os incidentes de segurança mais ocorridos nos setores financeiro, governamental, saúde, industrial, outros, de telecomunicação e transporte, respectivamente. Destaque para o *rasomware* no transporte e na área da saúde, para o vazamento de dados nas telecomunicações e para o furto de dinheiro na área financeira.

---

[335] KASPERSKY. **Incident response analyst report**. 2021. Disponível em: https://securelist.com/the-nature-of-cyber-incidents/107119/

[336] KASPERSKY. **Incident response analyst report** 2021. Disponível em: https://securelist.com/the-nature-of-cyber-incidents/107119/ 4 p.

[337] "*Ransomware* é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo. Na maioria dos casos, a infecção por *ransomware* ocorre da seguinte maneira. O malware primeiro ganha acesso ao dispositivo. Dependendo do tipo de *ramsomware*, todo o sistema operacional ou apenas arquivos individuais são criptografados. Um resgate é, então, exigido das vítimas". KASPERSKY. **Ransomware: definição, prevenção e remoção.** Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware

Na Europa, a *European Union Agency for Cybersecurity* (ENISA) é a entidade responsável por formular relatórios de incidentes de segurança da UE para setores específicos. Há mais de uma década, a ENISA, junto com as autoridades nacionais dos Estados-Membros da União Europeia, recolhe e analisa relatórios de incidentes de segurança nas telecomunicações[338].

Em julho de 2022, foi publicado o relatório de incidentes de segurança da área de telecomunicações relativo ao período de 2021. Segundo este relatório, ocorreram 168 incidentes em 26 Estados-membros e de 2 países da *European Free Trade Association* (EFTA). Ainda, foi feita uma comparação entre o número de incidentes ocorridos nos anos anteriores, mostrando leve queda de ocorrências em relação a 2020, mas um aumento em comparação com os anos anteriores[339].

Pela primeira vez, foi constatada ocorrências de incidentes relativos à confidencialidade e autenticidade. Três grandes incidentes foram relatados em 2021 e a ENISA calcula que esse número irá crescer nos próximos anos[340].

Atualmente, o foco das autoridades nacionais de segurança em telecomunicações dos países que constituem a União Europeia está na implementação do *European Electronic Communications Code* (EECC)[341]. Este novo conjunto de regras de implantação de redes de fibra e 5G objetiva harmonizar as regras do setor em toda UE, além de promover a implantação de tecnologia IoT e de novos modelos de negócios[342].

Já no Brasil, ocorreu um aumento significativo dos comunicados de incidentes de segurança para a ANPD. Segundo o relatório do ciclo de monitoramento do exercício de 2022, a ANPD recebeu, até dezembro de 2022, 473 comunicados de incidentes de segurança, do qual 297 foram recebidos em 2022 e 186 em 2021, representando um aumento de 56%[343].

---

[338]ENISA. **Telecom Security Incidents** *2021.* 27/07/2022. Disponível em: https://www.enisa.europa.eu/publications/telecom-security-incidents-2021. P 6

[339]ENISA. **Telecom Security Incidents** *2021.* 27/07/2022. Disponível em: https://www.enisa.europa.eu/publications/telecom-security-incidents-2021. P 4

[340]ENISA. **Telecom Security Incidents** *2021.* 27/07/2022. Disponível em: https://www.enisa.europa.eu/publications/telecom-security-incidents-2021. P 5

[341] EUROPEAN UNION LAW. **Directiva (UE) 2018/1972 Do Parlamento Europeu e Conselho de 11 de dezembro de 2018**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018L1972

[342]ENISA. **European Electronic Communications Code** Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-policy/european-electronic-communications-code

[343] BRASIL. Autoridade Nacional de Proteção de Dados. **Publicado relatório do ciclo de Monitoramento da ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/publicado-relatorio-do-ciclo-de-monitoramento-da-anpd 23 p.

Diante dos panoramas de ocorrências de incidentes de segurança em escalas globais, regionais e no Brasil, passa a verificar casos sobre o assunto. Por questão didática, primeiramente, serão tratados casos no mundo e, após, no Brasil.

Em 2017, ocorreu um ataque de *phishing*[344] contra *Torrance Memorial Medical Center,* hospital privado localizado em Torrance, na Califórnia.[345]As autoridades descobriram acessos não autorizados a duas contas de e-mails do hospital. Foi confirmado que haviam informações pessoais de pacientes nos e-mails violados, como nomes, datas de nascimento, números de registros médicos, números de seguro social e outras informações de diagnóstico.

O hospital comunicou o incidente ao Departamento de Saúde e Serviços Humanos dos EUA, ao Departamento de Saúde da Califórnia e ao FBI. Não se sabe quantas pessoas foram afetadas e nem o volume de dados que foram vazados[346].

Em 2019, ocorreu um incidente de violação de dados no banco norte-americano *Capital One*, uma das maiores instituições financeiras dos Estados Unidos. Um indivíduo externo conseguiu acesso não autorizado a informações pessoais de diversos clientes do cartão de crédito *Capital One*, além de outras pessoas que solicitaram os produtos do cartão de crédito[347].

Segundo o banco, este crime afetou 100 milhões de clientes que residem nos EUA e 6 milhões de clientes que se encontram no Canadá. Alguns dos dados acessados foram e-mails, data de nascimento, número de telefone, endereços e renda declarada pelo titular.

O banco informou que o criminoso foi encontrado pelo FBI. Após investigações, o governo americano alegou que os dados foram recuperados e que não há provas de que os dados foram compartilhados ou utilizados em crimes de fraude.

Em 2018, o hospital do Barreiro, no distrito de Setúbal, Portugal, recebeu uma multa de 400 mil euros da Comissão Nacional de Proteção de Dados (CNPD) por acesso irregular aos

---

[344] "Os ataques de *phishing* são exercidos por golpistas disfarçados de fontes confiáveis para facilitar o acesso a todos os tipos de dados confidenciais. Existem vários tipos de *phishing*, sendo alguns deles o e-mail de *phishing,* o *phishing* de malware e o *whaling*", MICROSOFT. **O que é phishing?** Diponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-phishing

[345] DAVIS, Jessica. **Phishing attack on Torrance Memorial puts patient records at risk.** Healthcare IT News. 20/60/2017. Disponível em: https://www.healthcareitnews.com/news/phishing-attack-torrance-memorial-puts-patient-records-risk.

[346] MADNICK, Stuart; NETO, Nelson Novais; BORGES, Natasha Malara; PAULA, Anchises Moraes G. de. **Developing a Global Data Breach Database and the Challenges Encountered.** Association for computing machine. Digital Library. 15/01/2021 Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. 28 p.

[347]CAPITAL ONE. **Information on the Capital One cyber incident.** Disponível em: https://www.capitalone.com/digital/facts2019/

dados dos pacientes. Duas das infrações foram o acesso indiscriminado de um conjunto de dados por profissionais e a ausência de medidas para impedir este acesso ilícito[348].

No mesmo ano, o aplicativo alemão *Knuddels* foi multado em 20 mil euros por violação do GDPR. Considerou-se que o aplicativo não tem mecanismos de segurança robustos para proteger os dados pessoais dos seus usuários[349].

Knuddels deixou as informações de seus usuários descriptografadas, facilitando o acesso de criminosos. Desse modo, mais de 300.000 credenciais de login foram comprometidas. Todavia, por conta da sua estratégia eficaz de resposta à violação dos dados, *Knuddels* foi poupada de uma multa maior.

No ano de 2019, a *National Revenue Agency* (NRA), agência fiscal da Bulgária, teve os dados pessoais de 5 milhões de cidadãos búlgaros afetados[350], totalizando 21 gigabytes de dados. Foram vazados vários tipos de dados pessoais como registros de salários e receitas, informações de segurança social, dívidas pessoais e pagamentos de saúde e pensões[351].

A investigação constatou que os responsáveis pelo tratamento de dados pessoais não tomaram medidas técnicas e organizacionais suficientes para limitar o ataque, além de não terem realizado uma avaliação de risco adequada para as suas operações de processamento de dados.

A Autoridade de Proteção de Dados da Bulgária aplicou uma multa de 2,6 milhões de euros para a NRA. Para além da multa, o *Global Forum on Transparency and Exchange of information for Tax Purposes* interrompeu a troca de informações com a Bulgária[352].

Em setembro de 2020, *Cosmote Mobile Telecommunications*, a maior operadora móvel da Grécia, sofreu um ataque de engenharia social[353]. Este ataque expôs dados pessoais dos

---

[348] PÚBLICO. **Hospital do Barreiro contesta judicialmente coima de 400 mil euros de Comissão de Dados.** 22/10/2018. Disponível em: https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479

[349] IRWIN, Lucas. **Chatt app Knuddles fined £20.000 for GDPR breach. IT Governance**. 29/11/2018. Disponível em: https://www.itgovernance.eu/blog/en/chat-app-knuddels-fined-e20000-for-gdpr-breach

[350] REPUBLIC OF BULGARIA. **Comission for Personal Data Protection. Information about CPDP's actions in relation to the personal data protection security breach at the National Revenue Agency.** 21/08/2019. Disponível em: https://www.cpdp.bg/en/index.php?p=news_view&aid=1505

[351] REPUBLIC OF BULGARIA**. Comission for Personal Data Protection. Update on the undertaken inspection at the National Revenue Agency**. 29/08/2019. Disponível em: https://www.cpdp.bg/en/?p=news_view&aid=1519

[352] REPUBLIC OF BULGARIA**. Comission for Personal Data Protection. Update on the undertaken inspection at the National Revenue Agency.** 29/08/2019. Disponível em: https://www.cpdp.bg/en/?p=news_view&aid=1519.

[353] Engenharia social na segurança cibernética é uma forma de enganar as pessoas para conseguir informações privadas que podem ser úteis para um ataque cibernético. Há vários meios de ataques de engenharia social, como e-mails ou mensagens de texto com links que levam a sites maliciosos. Outro exemplo é um telefonema de um cibercriminoso que finge ser do suporte técnico de um banco e solicita informações confidenciais. Para mais informações: TUNGGAL, Abi Tyas. **What is Social Engineering? Definition + Attack Examples**. Up Guard. 06/04/2023. Disponível em: https://www.upguard.com/blog/social-engineering.

clientes da operadora, tendo um impacto em 4,8 milhões de clientes e 48GB de dados roubados[354].

As investigações concluíram que a operadora estava processando dados de clientes de forma diversa do que determina o GDPR. Parte dos dados pessoais comprometidos não foram criptografados, o que facilitou a ação dos hackers. Para piorar, a operadora não notificou os titulares que tiveram os seus dados violados, contrariando, mais uma vez, o GDPR.

Desse modo, a *Cosmote Mobile Telcommunications* foi multada em 6 milhões de euros pela *Hellenic Data Protection Authority* – HDPA. Como se não bastasse, também foi multada em 3,25 milhões de euros por faltas de medidas de segurança e de infraestrutura de segurança cibernética[355].

No Brasil, em 2021, o Banco Central confirmou o vazamento de dados de 395 mil chaves PIX que estavam sob a custódia do BANESE (Banco do estado do Sergipe). Segundo o BC, as falhas ocorreram em sistemas da instituição financeira, mas não houve o vazamento de dados sensíveis como senhas, informações de movimentação e saldos financeiros[356].

Após estas falhas, o BC anunciou, no mesmo ano, medidas de segurança no PIX. Entre elas estão o limite de valor transferido durante a noite, o envio de notificações de transações rejeitadas por suspeita de fraude e mecanismos adicionais para a proteção de dados[357].

No ano de 2023, o Banco Central anunciou novas medidas de segurança[358]. Uma delas foi o aprimoramento das informações armazenadas pelo Banco Central, compartilhando-as com as demais instituições financeiras para evitar fraude.

Outro caso ocorrido no Brasil foi a operação *Deepwater,* em que a ANPD solicitou à Polícia Federal que investigasse o vazamento de dados de mais de 223 milhões de brasileiros – número superior à população do país – tendo em vista que também foram vazados dados de pessoas falecidas[359]. Segundo a PF, em 2021, inúmeros dados sigilosos de pessoas físicas e

---

[354]ONE TRUST DATAGUIDANCE. **Greece. HDPA fines Cosmote £6M for data breach and unlawful data processing.** Regulation Research software. 01/02/2022**.** Disponível em: https://www.dataguidance.com/news/greece-hdpa-fines-cosmote-6m-data-breach-and-unlawful

[355]EKATHIMERINI. **Mobile phone operator slapped with fine over data breach.** Disponível em: https://www.ekathimerini.com/economy/1176648/mobile-phone-operator-slapped-with-fine-over-data-breach/

[356] BASÍLIO, Patrícia. **BC confirma vazamento de 395 mil chaves PIX sob responsabilidade da BANESE** . G1 Portal de notícias da Globo. 30/09/2021. Disponível em:. https://g1.globo.com/economia/noticia/2021/09/30/bc-confirma-vazamento-de-395-mil-chaves-pix-de-clientes-do-banese.ghtml

[357]BANCO CENTRAL DO BRASIL. **BC aprimora mecanismos de segurança do PIX.** 29/09/2021. Disponível em: https://www.bcb.gov.br/detalhenoticia/581/noticia

[358]BANCO CENTRAL DO BRASIL. **BC aprimora mecanismos de segurança do PIX**.02/05/2023. Disponível em: https://www.bcb.gov.br/detalhenoticia/677/noticia

[359]PORTAL DE NOTÍCIAS DA GLOBO. **Hacker preso por megavazamento de dados tem 24 anos e vive em Uberlândia; ele também é suspeito de invadir o Senado, o Exército e o TSE.** Disponível em:

jurídicas foram ilicitamente disponibilizados em um fórum na internet de trocas de informações sobre atividades cibernéticas[360].

Em 2023, o Ministério da Saúde anunciou um registro de incidentes com dados pessoais em alguns sistemas governamentais, entre eles, o e-SUS notifica e o CADSUS (Sistema de Cadastramento de Usuários do Sistema Único de Saúde). Segundo o governo, houve a ocorrência de crime cibernético de venda ilegal de base de dados desses sistemas[361].

Não foi possível afirmar quais foram os dados comercializados ilegalmente. Todavia, segundo o Ministério da Saúde, não houve identificação de prejuízos para os titulares e nem a exposição dos seus CPFs.

Diante de todos esses incidentes, foram identificados obstáculos para potencializar a segurança dos dados. As divergências entre regulamentações de segurança cibernética e a dificuldade em mapear os incidentes de segurança, como o *modus operandi* dos ataques[362], representam dois desses obstáculos.

Outra dificuldade encontrada é a falta de padrões globais uniformes para determinar os procedimentos de segurança em escala global, haja vista a abrangência internacional de várias tecnologias. Muitos países e empresas ainda não possuem padrões rígidos de proteção eficazes dos dados pessoais dos usuários nem métodos eficientes de comunicação para informar sobre a ocorrências de violações.[363]

Estes problemas estão diretamente ligados a cidades inteligentes, dada a complexidade do seu ambiente, formado com vários produtos e serviços de origens diferentes. Como citado anteriormente, a União Europeia, por meio da *European Electronic Communications Code* (EECC), busca padronizar os sistemas de segurança do setor de telecomunicações entre os seus países membros.

As cidades inteligentes possuem a característica de integrar toda a tecnologia de informação e comunicação (TIC) e inovações para lidar com dados complexos em dispositivos

---

https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/19/suspeito-do-maior-vazamento-de-dados-do-brasil-e-preso-em-uberlandia.ghtml

[360]POLÍCIA FEDERAL. **Polícia Federal deflagra Operação Deepwater que combate a obtenção e vazamento ilegal de dados pessoais de brasileiros pela internet**. 29/03/2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/03/policia-federal-deflagra-a-operacao-deepwater-que-combate-a-obtencao-e-vazamento-ilegal-de-dados-pessoais-de-brasileiros-pela-internet

[361]MINISTÉRIO DA SAÚDE. **Registros de Incidentes com dados pessoais**. Disponível em*:* https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais

[362]MADNICK, Stuart; NETO, Nelson Novais; BORGES, Natasha Malara; PAULA, Anchises Moraes G. de. **Developing a Global Data Breach Database and the Challenges Encountered**. Association for computing machine. Digital Library. 15/01/2021 Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. 3 p.

[363] MADNICK, Stuart; NETO, Nelson Novais; BORGES, Natasha Malara; PAULA, Anchises Moraes G. de. **Developing a Global Data Breach Database and the Challenges Encountered**. Association for computing machine. Digital Library. 15/01/2021 Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873 2 p.

de armazenamento, além de transmiti-los por toda a cidade. No entanto, dados pessoais estão sob risco de vários ataques, pois o sistema de segurança de muitas tecnologias implantadas nas cidades inteligentes ainda não são confiáveis[364].

A segurança e a privacidade da TIC são essenciais, não só para os dados pessoais e para a privacidade, mas também para o funcionamento dos elementos inteligentes da cidade como, edifícios, fábricas, sistemas de saúde e transporte. Os sistemas de IoT ainda precisam desenvolver a segurança *antimalware* adequada para funcionar 24 horas por dia, durante 7 dias por semana[365].

Conforme se extrai das análises de caso abordadas, é importante ter cautela na implantação de cidade inteligente, a despeito da falta de padronização das normas de segurança e da limitação tecnológica em garantir a proteção exigida pelas legislações. Com efeito, além do risco de violações aos direitos do cidadão, as empresas de TIC e entidades governamentais podem ser punidas por meio de multas com altos valores, impostas pelas Autoridades de Proteção de Dados.

2.8. Monitoramento excessivo, discriminação e fruição de dados pessoais

O último tópico do capítulo 1 aborda os problemas de monitoramento excessivo e discriminação no ambiente tecnológico urbano, por meio de casos concretos ocorridos no estrangeiro e no Brasil. Especialmente, analisa as discussões entre os direitos e as liberdades do cidadão e a potencialização da prestação de serviços públicos.

Governos demandam das empresas comerciais o compartilhamento de dados pessoais dos seus clientes para fins de interesse público, como inquéritos criminais e segurança nacional[366]. Porém, com o advento de ordenamentos jurídicos que concretizaram a proteção aos direitos de privacidade e de dados pessoais, as empresas devem ter cautela no compartilhamento desses dados, equilibrando os interesses envolvidos.

Ademais, nas cidades inteligentes, também ocorre a situação inversa que é o acesso a banco de dados governamentais pelas empresas privadas de tecnologia que prestam serviços públicos. Neste caso, o governo deve controlar e fiscalizar o acesso dessas empresas, que devem

---

[364] VORAKULPIPAT, Chalee; KO, Ryan K. L.; LI, Qi; MEDDAHI, Ahmed. **Security and Privacy in Smart Cities** 15/08/2021. HINDAWI. Disponível em: https://www.hindawi.com/journals/scn/si/403673/

[365] VORAKULPIPAT, Chalee; KO, Ryan K. L.; LI, Qi; MEDDAHI, Ahmed. **Security and Privacy in Smart Cities** 15/08/2021. HINDAWI. Disponível em: https://www.hindawi.com/journals/scn/si/403673/

[366] CATE, Fred H. DEMPSEY, James X. **Bulk *Collection*: Systematic Government Access to Private- Sector Data.** OXFORD. 2017. 6 p.

coletar o mínimo de dados pessoais possível, usá-los somente para as finalidades legais pactuadas e adotar medidas protetivas eficazes.

É inequívoca a importância desse tema para a implantação de *smart city*, uma vez que há um sério risco de violação a vários direitos fundamentais dos cidadãos, especialmente contra a privacidade, a igualdade, a inclusão social, a liberdade e a não discriminação. A falta de uma regulamentação adequada para determinadas situações envolvendo tecnologia, proteção de dados e privacidade também justifica a importância desse estudo.

Antes de mais nada, reitera que a inovação tecnológica traz grandes benefícios para a sociedade e, portanto, deve ser incentivada. O que se busca neste trabalho é a observância dos direitos do cidadão na implantação da tecnologia em cidades.

O monitoramento eletrônico em massa é um processo que ocorre durante a utilização da tecnologia para monitorar comportamentos, e tem como propósito, ao menos aparente, potencializar algum serviço público, a exemplo da segurança. Esse tipo de monitoramento pode ser realizado tanto por empresas privadas como por órgãos governamentais.

Há várias formas de realizar o monitoramento eletrônico em massa, como, por meio de sistemas de vigilância, câmeras, sensores de áudio e imagem e banco de dados de coleta e processamento de informações. Inicialmente, analisa o *Systematic Access,* monitoramento eletrônico realizado por entidade governamental através do acesso ao banco de dados de uma empresa privada.

Geralmente, o *Systematic Access* é legitimado sob o argumento de segurança nacional. O pretexto da proteção estatal para ter acesso ao banco de dados de terceiros ganhou força depois dos atentados de 11/09/2001, em Nova York.

A prática do *Systematic Access* coloca os controladores de dados em uma situação delicada, pois recaem sobre eles a responsabilidade de decidir sobre questões como a natureza, licita ou ilícita, do pedido do governo e se essa demanda deve ser informada ao titular dos dados, em respeito ao princípio da transparência. Por motivos óbvios, é interessante para os governantes a ausência de legislações com regras claras e objetivas que limitam o seu direito de acesso aos bancos de dados das entidades privadas.

Portanto, ficam a cargo do judiciário e da doutrina de cada país a criação de salvaguardas para determinados abusos. Um episódio emblemático sobre a prática do *Systematic Access* ocorreu em 2011, nos Estados Unidos, no caso intitulado *Carpenter v. United States.*[367]

[367]UNITED STATES OF AMERICA Supreme court of the United States. **CARPENTER v. UNITED STATES**. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Em breve síntese, o governo americano teve acesso, através de uma ordem judicial, aos registros de localização dos celulares de vários suspeitos de cometer roubos na cidade de Detroit, estado de Michigan, e, entre eles, estava Timothy Carpenter. Por conta dos dados de localização obtidos, o governo americano demonstrou que o celular de Carpenter estava próximo dos locais dos crimes no momento em que eles ocorreram.

A ordem judicial que concedeu o acesso aos registros de localização se baseou em uma lei chamada popularmente de *Stored Communications act*, que impõe a divulgação obrigatória de comunicações eletrônicas armazenadas por provedores de serviços de internet, quando essas informações são pertinentes para uma investigação criminal em curso. [368] Esta lei facilita a emissão de um mandado judicial, pois retira a exigência do fundamento da *causa provável*, requisito geral para a expedição de mandados judiciais nos EUA[369]

A defesa de Carpenter interpôs recurso perante a Corte de Apelação do Sexto Circuito,[370] com base na quarta emenda constitucional americana, que visa proteger as pessoas de buscas e apreensões consideradas infundadas perante a lei[371]. O recurso foi negado e Carpenter foi condenado.

O motivo da negativa do recurso foi que a Corte não caracterizou como busca a consulta do governo americano sob os registros históricos de telemóveis. Com isso, não foi considerado que Carpenter poderia ter uma expectativa razoável de privacidade e, portanto, o réu não teve direito de ser protegido pela Quarta Emenda.

O argumento sustentado pela Corte foi que Carpenter havia compartilhado voluntariamente as suas informações sobre a sua localidade com as operadoras de telefonia móvel e, por isso, não poderia ter expectativas razoáveis de privacidade. Segundo o tribunal, se o usuário transmitiu os dados do seu celular para a sua operadora como forma de estabelecer

---

[368] UNITED STATES OF AMERICA. US CODE. **Stored Communications act** . Title 18. Part 1. Chapter 121 §2701 Disponível em: https://uscode.house.gov/view.xhtml?req=(title:18%20section:2701%20edition:prelim)

[369] *2. The Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show "reasonablegrounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U. S. C. §2703(d). That showing fallswell short of the probable cause required for a warrant. Consequently, an order issued under §2703(d) is not a permissible mechanism foraccessing historical cell-site records. Not all orders compelling theproduction of documents will require a showing of probable cause.* UNITED STATES OF AMERICA Supreme court of the United States **CARPENTER v. UNITED STATES.** Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf 3 p.

[370] Tribunal Federal que exerce a sua jurisdição em quatro estados americanos, sendo eles Michigan, Kentucky, Ohio e Tennesse. UNITED STATES OF AMERICA United States Court of Appeals for de Sixth Circuit. **About the court.** Disponível em: https://www.ca6.uscourts.gov/about-court

[371] UNITED STATES COURT. *What does the Fourth Amendament Mean?* Disponível em: https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0#:~:text=The%20Constitution%2C%20through%20the%20Fourth,deemed%20unreasonable%20under%20the%20law.

comunicação, então esse ato não pode ser protegido pela Quarta Emenda Constitucional Americana.[372]

Este entendimento teve como alicerce doutrinário a *third-party doutrine*, um princípio jurídico americano desenvolvido a partir de decisões judiciais. Este princípio consiste na perda da expectativa de privacidade quando o titular das informações as compartilha com um terceiro[373].

Na era digital, o princípio do *third-party doutrine* pode ocasionar profundas implicações na privacidade. Em uma situação hipotética, uma casa inteligente pode ser autorizada pelo usuário a compartilhar os seus dados para terceiros fornecedores de serviços. Nesse caso, a justiça pode entender pela retirada da expectativa de privacidade do morador e, por consequência, pela remoção da proteção da Quarta Emenda[374].

A decisão da Corte de Michigan foi levada para a Suprema Corte Americana, que a reverteu por maioria de votos, mantendo o direito de Carpenter de invocar a Quarta Emenda. A Suprema Corte decidiu que o progresso da ciência como ferramenta poderosa utilizada no cumprimento de deveres estatais não pode oferecer acesso irrestrito ao Estado à banco de dados de informações.

Desse modo, a Suprema Corte considerou que, no caso de Carpenter, houve acesso infundado do Estado ao banco de dados de registro de localização, uma vez que esse acesso foi caracterizado como busca e, portanto, exigiu-se o cumprimento do requisito da *causa provável* para a emissão da ordem judicial. Ademais, em um dos votos foi mencionado que a forma automática da recolha dos dados por terceiros não é motivo para o afastamento da Quarta Emenda[375].

Este caso mostra a dificuldade de limitar o acesso do Estado a todo tipo de informações, mesmo aquelas confidenciais ou sensíveis. Aqui, nota-se a real necessidade de regular o acesso estatal ao banco de dados de terceiros, já que o governo pode utilizar de teorias jurídicas, como

---

[372] UNITED STATES OF AMERICA Supreme court of the United States. **CARPENTER v. UNITED STATES.** Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf 8 p.

[373] GORIN, Eisner. **The third-party doctrine and the fourth amendment.** 08/12/2023. Disponível em https://www.thefederalcriminalattorneys.com/third-party-doctrine

[374] GORIN, Eisner. **The third-party doctrine and the fourth amendment**. 08/12/2023. Disponível em https://www.thefederalcriminalattorneys.com/third-party-doctrine

[375] "We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment. UNITED STATES OF AMERICA Supreme court of the United States". **CARPENTER v. UNITED STATES.** Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf 26 p.

foi o caso da *third-party doutrine,* para justificar práticas que violam os direitos dos titulares dos dados.

Na cidade do Rio de Janeiro, o juízo de primeiro grau determinou à Google que concedesse ao Ministério Público dados dos seus usuários que estavam nos arredores do lugar do crime de homicídio contra Marielle Franco, até então vereadora, e Anderson Gomes, seu motorista. A determinação consistiu no fornecimento de dados daqueles usuários que tivessem algo relacionado à ex-vereadora, como, por exemplo, alguém que pesquisou o nome de Marielle Franco, por qualquer motivo, e que estava próximo do lugar do crime no momento em que ele ocorreu [376].

A imposição do juízo de primeiro grau abrangeu fornecimento de dados desses usuários pelo período de 2 anos. As informações consistiam em: dados de identificação de conta de usuário e dados cadastrais; registros de conexão (IPs); Mídia (fotos, vídeos e outros); históricos de pesquisa, de navegação e de localização; e-mails; agenda e agenda de contatos[377].

A referida decisão foi impugnada pela Google e chegou à sexta turma do Superior Tribunal de Justiça. Na impugnação, a Google contestou três pontos da decisão, sendo eles: o número indeterminado de cidadãos que seriam afetados em seus direitos de privacidade e liberdade de comunicação, além da violação ao princípio da presunção de inocência; os tipos de dados que seriam fornecidos ao Ministério Público e; o longo prazo fornecido de dois anos de histórico de cada um desses cidadãos[378].

A Google alegou que a quebra do sigilo de dados deve ocorrer apenas para pessoas suspeitas e que serão investigadas, conforme preceitua o artigo 5º incisos IX, X, e XI da Constituição Brasileira. Ainda, afirmou sobre a inexistência de previsão no ordenamento jurídico brasileiro quanto ao fornecimento indiscriminado de dados de um número indeterminado de pessoas que simplesmente buscaram informações sobre a vítima na internet[379].

---

[376]ABRUSIO, Juliana; MARANHÃO, Juliano; CAMPOS, Ricardo; LÓPEZ, Nuria. **Dados de Geolocalização e a investigação de Marielle Franco.** 07/07/2020. Disponível em: https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle/

[377] BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 64.941-RJ** (2022/0284473-3). Agravante: G.B.I. L. e outros. Agravado: Ministério Público do Estado do Rio de Janeiro. Relator: Ministro Rogério Schietti Cruz. Brasília, 18 de abril de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1262917027/inteiro-teor-1262917112 6 p.

[378] BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 64.941-RJ** (2022/0284473-3). Agravante: G.B.I. L. e outros. Agravado: Ministério Público do Estado do Rio de Janeiro. Relator: Ministro Rogério Schietti Cruz. Brasília, 18 de abril de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1262917027/inteiro-teor-1262917112 7 p.

[379] BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 64.941-RJ** (2022/0284473-3). Agravante: G.B.I. L. e outros. Agravado: Ministério Público do Estado do Rio de Janeiro. Relator: Ministro

Por maioria de votos, a 6ª Turma do STJ negou o agravo regimental da Google, impondo à empresa que realizasse o fornecimento das informações na forma estabelecida pela sentença de primeiro grau, sob pena de multa diária milionária, em caso de omissão. Dentre os argumentos que basearam a decisão do STJ estão a supremacia do interesse público sobre os interesses individuais ou coletivos e a necessidade da medida para fins de investigação criminal, uma vez que não há direito absoluto previsto pela Constituição Brasileira.

Em seu voto vencido, o ministro Sebastião Reis Jr. considerou que há violação à privacidade no acesso do MP a registros de agenda, aplicativos, mídias e históricos de navegação e pesquisa dos usuários da Google. Ainda, o ministro entendeu que o período de dois anos de informações dos usuários era descabido e desproporcional, não havendo razão plausível para tal medida.

Antes de mais nada, destacam-se os esforços do MP, louváveis e pertinentes, para investigar o assassinato de Marielle Franco e de Anderson Gomes. No entanto, a forma como ocorreu, especificamente, a liberação de informações privadas que estavam em posse de terceiro, é descabida, desproporcional e viola vários direitos, especialmente sobre a privacidade e a liberdade de expressão, e princípios, como a presunção da inocência.

O que mais chama atenção na decisão mantida pelo STJ é a liberação de informações de pessoas que sequer tenham ligação com as investigações, bem como os 2 anos de conteúdo fornecido dessas pessoas ao MP. Esta decisão já seria questionável se as informações pertencessem a suspeitos investigados, como ocorreu no caso Carpenter v. United States, já discutido neste trabalho.

Este precedente jurisprudencial é mais perigoso que o precedente americano, haja vista que, além de ter o aval de um tribunal superior, houve a violação de direitos de um grupo indeterminado de pessoas. A questão não se trata especificamente do assassinato de Marielle Franco, a que muito interessa encontrar os culpados, mas, na ação do Estado de infringir direitos e princípios constitucionais de forma descabida, desproporcional e sem uma justificativa aceitável.

A finalidade da medida aprovada pelo STJ é a segurança pública, mas, sequer há certeza de que a busca por informações contidas nos registros da Google irá atingir os objetivos da investigação. Todavia, existe a certeza de que direitos como a privacidade de cidadãos inocentes serão violados.

Rogério Schietti Cruz. Brasília, 18 de abril de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1262917027/inteiro-teor-1262917112 13 p.

Outro caso que merece menção são as ações penais advindas dos atos antidemocráticos ocorridos no dia oito de janeiro de 2023, em Brasília. O STF recebeu 1345 denúncias, sendo que 232 denúncias foram classificadas como crimes mais graves, entre eles, associação criminosa armada, abolição violenta do Estado Democrático de Direito e tentativa de golpe de Estado. [380].

Em setembro de 2023, o ministro relator Alexandre de Moraes divulgou um balanço[381] dos processos relacionados aos atos antidemocráticos de 08/01 do qual houve diversas medidas cautelares relativas a 143 buscas e apreensões, 808 afastamentos de sigilo bancário e 8 afastamentos de sigilo telemático[382].

A época da confecção deste trabalho, as ações ainda seguem em andamento (inclusive em segredo de justiça) e há um vasto conteúdo da inteligência brasileira que não foi revelado. Portanto, não se sabe exatamente quais são as provas que servem de base para os processos penais, como elas foram adquiridas e quais os argumentos para a concessão.[383] Posteriormente, importa investigar se houve medidas contra a proteção de dados pessoais e a privacidade.

Na cidade de São Paulo, o Instituto Brasileiro de Defesa ao Consumidor (IDEC) moveu uma ação pública contra a Via Quatro, concessionária da Linha Amarela do Metrô de São Paulo. O IDEC requereu a proibição da coleta e do tratamento de dados biométricos dos usuários sem autorização prévia e uma indenização pelo uso indevido de câmeras de segurança de captação de imagens para fins comerciais e publicitários.

A Via Quatro foi condenada, em primeira instância, a pagar uma indenização de R$ 100.000,00, por dano moral coletivo, e proibida de usar as imagens sem a autorização dos usuários. Em 2023, o órgão colegiado do Tribunal de Justiça de São Paulo aumentou o valor da indenização da concessionária em R$ 500.000,00, revertido para o Fundo de Defesa dos Direitos Difusos[384].

---

[380]BRASIL. Superior Tribunal Federal. **STF condena mais cinco réus pelos atos antidemocráticos de 8/1.** 25/10/2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=518984&ori=1

[381] BRASIL. Superior Tribunal Federal. **Relator divulga balanço dos processos relacionados aos atos antidemocráticos de 8/1.** 13/09/2023 Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=513973&ori=1

[382] "A quebra de sigilo telemático é uma medida adotada para solicitar dados de usuários de serviços eletrônicos, a fim de identificar e coletar informações de certo indivíduo suspeito de cometimento de crime, mediante autorização judicial." VAZ, Bruna; ZOMBARDI, José Lucas; GUEIROS, Pedro. **O caso "Google x Marielle Franco" e a quebra do sigilo telemático genérica.** Consultor jurídico. 26/10/2023. Disponível em: https://www.conjur.com.br/2023-out-26/opiniao-google-marielle-franco-quebra-sigilo-telematico-generica/#:~:text=Para%20melhor%20compreens%C3%A3o%2C%20a%20quebra,de%20crime%2C%20mediante%20autoriza%C3%A7%C3%A3o%20judicial.

[383] BRASIL. Superior Tribunal Federal. **Entenda a condenação dos réus pelos atos antidemocráticos de 8 de janeiro**. 25/10/2023 https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=517059&ori=1

[384] TRIBUNAL DE JUSTIÇA DE SÃO PAULO. **TJSP mantém proibição de coleta de dados pela Via Quatro.** 10/05/2023. Disponível em**:** https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=91605&pagina=1

Na passagem do ano de 2023 para 2024, foram instaladas câmeras de reconhecimento facial na cidade do Rio de Janeiro, especificamente na Barra da Tijuca e em Copacabana. O banco de dados desse sistema continha um mandado de prisão contra uma mulher que transitava nas ruas do bairro de Copacabana[385].

Assim que a mulher foi identificada pelas câmeras de reconhecimento facial, ela foi presa pela Polícia Civil. Após a prisão, os policiais verificaram que os dados do sistema de reconhecimento facial estavam desatualizados, pois o mandado de prisão contra a mulher já tinha sido cumprido. Logo em seguida, ela foi posta em liberdade.

A Secretaria de Segurança da cidade alegou que a Polícia tem a função de checar as informações, uma vez que pode ocorrer inconsistências no sistema de reconhecimento facial por conta da desatualização das informações em seu banco de dados. Este caso evidencia a importância do treinamento de servidores públicos no uso da tecnologia, especialmente para entenderem a limitação de cada sistema e realizarem medidas preventivas que minimizem erros.

Outra ação judicial americana importante é a disputa entre *American Civil Liberties (ACLU) v. Clapper.*[386] A ACLU ajuizou ação contra o governo federal dos Estados Unidos, representado na figura do diretor da Inteligência Nacional, *James Clapper*, por conta de um programa de coleta em massa de metadados telefônicos executado pela *National Security Agency* (NSA).

Desde as famosas revelações de Edward Snowden[387] sobre a vigilância em massa realizada pelo governo dos Estados Unidos, incluindo a espionagem sob chefes de outros Estados, foram intensificadas as discussões sobre a governança de dados. Os debates passam pelo direito de acesso do governo a banco de dados ou redes do setor privado, seja de forma direta ou por meio do compartilhamento de dados[388].

O programa da NSA coletava metadados sobre chamadas telefônicas e armazenava-os em um repositório que poderia ser acessado posteriormente. Apesar de não gravar o conteúdo da chamada, haviam detalhes, como, a sua duração, os números de telefone que fazia e recebia a chamada e onde a chamada foi feita.

---

[385]COELHO, Henrique; NASCIMENTO, Rafael; ALVES, Raoni. **Mulher presa após reconhecimento facial é solta**. Mandado de prisão já tinha sido cumprido. G1 Portal de notícias da Globo. 04/01/2024 Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/01/04/mulher-presa-apos-reconhecimento-facial-e-solta-mandado-de-prisao-ja-tinha-sido-cumprido.ghtml

[386]JUSTIA US LAW. **CLU v. Clapper.** No. 14-42 (2d Cir. 2015) Disponível em: https://law.justia.com/cases/federal/appellate-courts/ca2/14-42/14-42-2015-10-29.html

[387]THE GUARDIAN. **Snowden NSA files surveillance revaletions decoded.** 2013. Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

[388] CATE, Fred H. DEMPSEY, James X. **Bulk Collection: Systematic Government Access to Private- Sector Data**. OXFORD. 2017. 6 p.

Em 2013, a ACLU, juntamente com a *New York Civil Liberties Union* (NYCLU) ofereceram uma denúncia contra o governo federal, solicitando ao Tribunal Distrital que declarasse o programa de metadados inconstitucional. O argumento da denúncia foi que o programa excedeu aos limites concedidos pela *USA Freedom Act,* violando a Primeira e a Quarta Emendas Constitucionais Americanas.

O *Freedom Act* é uma lei que concedeu ao governo a permissão de coletar, por um período de 180 dias, registros de chamadas, em caso de suspeitas de terrorismo internacional. Esta lei exigia que requisitos fossem cumpridos para a coleta, além de procedimentos como a destruição imediata dos registros de chamadas que não fossem objeto de investigação terrorista.

A ACLU e a NYCLU também requereram uma liminar, perante a Corte de Apelação do Segundo Circuito, pedindo a proibição permanente da continuidade do programa. Por fim, a liminar também requereu que o governo não coletasse os registros de chamadas dos requerentes e colocasse em quarentena todos os registros de chamadas dos recorrentes já coletados pelo programa.

Como argumento de defesa., o governo federal dos Estados Unidos alegou, novamente, a *third-party doutrine.* Com base nessa teoria, os indivíduos não têm o direito de privacidade de registros entregues voluntariamente a provedores de telefonia terceirizados.

Ainda, o governo alegou que o período de 180 dias de funcionamento do programa, estabelecido pelo Congresso através da *Freedom act*, equilibrou os direitos à privacidade e à segurança nacional. O governo solicitou que o tribunal não abordasse questões de ordem constitucional e respeitasse a decisão do Congresso quanto a realização do programa pelo período previsto.

Em sua decisão, a Corte acatou a defesa do governo federal, mantendo o programa até o final do prazo de 180 dias determinados pela lei. Por conseguinte, a Corte não abordou as questões constitucionais, indagadas pela liminar, sobre o programa.

Este precedente judicial tem consequências negativas para o cidadão, pois foram violados vários direitos, entre eles a privacidade e a proteção dos dados pessoais, em prol da segurança nacional. Casos como este legalizam a vigilância estatal, estabelecida pelo congresso, executada pelo Estado e ratificada pela justiça.

As revelações de Snowden também identificaram programas de vigilância no Reino Unido, mostrando o envolvimento da Sede de Comunicações do Governo do Reino Unido em

uma operação denominada TEMPORA. O programa consistia em coletar e armazenar um enorme volume de dados que eram extraídos de cabos submarinos[389].

Este tipo de exploração é uma espécie de interceptação em massa de comunicações e permitiu a Sede de Comunicações de UK de armazenar grande volume de dados, filtrá-los por meio de critérios de seleção e examiná-los. Logo após a publicidade do programa TEMPORA, várias ONGs, entre elas a *Big Brother Wacth*, organizações sem fins lucrativos, acadêmicos e jornalistas representaram contra o governo do Reino Unido perante a Corte Europeia de Direitos Humanos[390].

Ao todo, foram apresentados três pedidos, sendo eles o *Big Brother Watch and Others v. the United Kington; Bureau of Investigative Journali*sm e *Alice Ross v the United Kington* e 10 *Human Rights Organizations and Others v. the United Kington.* Em todos os casos, houve a alegação de que o governo do Reino Unido violou o direito ao respeito pela vida privada, constante no artigo 8º da Convenção Europeia dos Direitos Humanos[391].

Todos os requerentes acreditavam que o serviço de inteligência do Reino Unido interceptava as suas comunicações eletrônicas por meio de técnicas de vigilância, a saber: pela interceptação em massa de comunicações sob a proteção da seção 8 da *Regulation of Investigatory Powers Act 2000* (RIPA)[392] do UK; o compartilhamento das informações com governos estrangeiros e; a obtenção de dados de comunicação pertencentes a prestadores de serviços de comunicações, na forma do capítulo II da RIPA[393].

No caso *Big Brother Watch and Others v. the United Kington*, houve reclamação quanto a incompatibilidade da RIPA com a Convenção Europeia dos Direitos Humanos. Ainda, argumentaram que não havia legalidade na interceptação de informações das agências de

---

[389] GLOBAL FREEDOM OF EXPRESSION. COLUMBIA UNIVERSITY. **Big Brother Watch v. Reino Unido.** Disponível em: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/

[390] EUROPEAN COURT OF HUMAN RIGHTS. **Big Brother Watch and others v the United Kingdom**. Disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13278%22]}

[391] "Art. 8° **Direito ao respeito pela vida privada e familiar** 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros". EUROPEAN COURT OF HUMAN RIGHTS. **Convenção Europeia dos Direitos do Homem**. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por

[392]UNITED KINGTOM. **Regulation of Investigatory Powers Act 2000**. Part 1. Chapter I, Interception warrants, Section 8. Disponível em:. https://www.legislation.gov.uk/ukpga/2000/23/section/8/enacted

[393]UNITED KINGTOM. **Regulation of Investigatory Powers Act 2000**. Part 1. Chapter II, Acquisition and disclosure of communications data. Disponível em:. https://www.legislation.gov.uk/ukpga/2000/23/part/I/chapter/II/enacted

inteligência estrangeiras e que as atividades violavam o seu direito à privacidade[394]. Por fim, alegaram que não havia um sistema de salvaguardas robusto e independente para controlar as formas de processamento e de interceptação de informações praticadas pelo governo do Reino Unido.

O Tribunal Europeu dos Direitos Humanos concluiu que um regime de interceptação em massa não era, por si só, incompatível com a Convenção Europeia de Direitos Humanos. No entanto, o Tribunal entendeu que o programa de interceptação em massa do Reino Unido violava a privacidade e a liberdade de expressão por conta de alguns motivos, entre eles, por falta de supervisão independente.

O Tribunal enfatizou a importância de um sistema de salvaguardas, que incluísse um controle exercido por órgãos independentes, com o propósito de proteger os direitos humanos e as liberdades fundamentais.[395] A supervisão ocorreria durante todo o processo de busca e de seleção do material a ser examinado pelo governo.

É notória a semelhança do *Big Brother Watch and Others v. the United Kingdom* com o caso *American Civil Liberties (ACLU) v. Clapper*, analisado anteriormente. Em ambas as situações houve a legalização de uma vigilância em massa praticada pelos governos do Reino Unido e dos EUA, respectivamente. Contudo, o caso nos EUA parece mais grave, haja vista a ratificação do judiciário.

É plausível a criação de uma autoridade independente para fiscalizar as ações de órgãos governamentais que estejam envolvidos com programas de monitoramento eletrônico em massa. Todavia, questiona se, em âmbito nacional, essa responsabilidade ficaria a cargo da ANPD ou de uma entidade específica a ser criada.

Quanto à Europa, também é interessante mencionar a Diretiva 2006/24 sobre retenção de dados, que foi editada após os atentados em Londres no ano de 2005. Essa diretiva obrigava as companhias de telecomunicações a manter, por um prazo de seis meses, os registros de dados pessoais de seus usuários[396].

---

[394]AMNESTY INTERNATIONAL **Big Brother Watch and others vs the United Kingdom** (Applications Nos. 58170/13, 62322/14 and 24960/15). 2018. Disponível em: https://policehumanrightsresources.org/big-brother-watch-and-others-vs-the-united-kingdom

[395] AMNESTY INTERNATIONAL **Big Brother Watch and others vs the United Kingdom** (Applications Nos. 58170/13, 62322/14 and 24960/15). 2018. Disponível em: https://policehumanrightsresources.org/big-brother-watch-and-others-vs-the-united-kingdom 127 p.

[396] VAZ, Bruna; ZOMBARDI, José Lucas; GUEIROS, Pedro. **O caso "Google x Marielle Franco" e a quebra do sigilo telemático genérica.** Consultor jurídico. 26/10/2023. Disponível em: https://www.conjur.com.br/2023-out-26/opiniao-google-marielle-franco-quebra-sigilo-telematico-generica/#:~:text=Para%20melhor%20compreens%C3%A3o%2C%20a%20quebra,de%20crime%2C%20mediante%20autoriza%C3%A7%C3%A3o%20judicial. 4 p.

O principal objetivo da diretiva 2006/24 era harmonizar as disposições dos Estados membros relativos à retenção de dados gerados ou processados por fornecedores de serviços, para garantir que estes dados estivessem disponíveis para fins de prevenção, investigação e repreensão de crimes graves[397]. A diretiva impunha a retenção de dados de tráfego, localização e dados relacionados a identificação do assinante, mas sem o conteúdo das comunicações[398].

A retenção indiscriminada de dados pessoais de número indeterminado de pessoas deu margem à violação de vários direitos dos cidadãos europeus[399]. Essa atuação de vigilância executada pelo Estado sobre os cidadãos ficou conhecida como *dragnet surveillance*[400].

Após a pressão de ativistas de direitos humanos, em abril de 2014, a Diretiva 2006/24 foi invalidada pelo Tribunal de Justiça da União Europeia, sob o fundamento da proteção à privacidade, considerando que a investigação indiscriminada de um número ilimitado de pessoas não poderia permanecer, mesmo quando o propósito era combater crimes graves como o terrorismo[401]. A decisão também destacou que a diretiva não garante um nível alto de segurança dos dados nem a sua destruição irreversível no final do período de retenção.

Em sua conclusão, o tribunal alegou que a diretiva não prevê meios suficientes para garantir a proteção eficaz dos dados contra os riscos de abuso, acesso ilegal ou uso ilegal dos dados retidos. Por fim, a decisão considerou que a Diretiva não estabelece regras claras sobre as interferências nos direitos fundamentais consagrados pelos artigos 7 e 8 da Carta de Direitos Fundamentais da União Europeia que tratam, respectivamente, do respeito a vida privada e familiar e da proteção de dados pessoais[402].

---

[396] BRASIL. Superior Tribunal Federal. **Entenda a condenação dos réus pelos atos antidemocráticos de 8 de janeiro.** 25/10/2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=518984&ori=1

[397] EUROPEAN UNION LAW. **Directive 2006/24/EC.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1405060274756&uri=CELEX:32006L0024

[398] CCDCOE. **EU Data Retention Directive Union.** Disponível em: https://ccdcoe.org/incyder-articles/eu-data-retention-directive-invalid/#footnote_1_2661

[399] CCDCOE. **EU Data Retention Directive Union.** Disponível em: https://ccdcoe.org/incyder-articles/eu-data-retention-directive-invalid/#footnote_1_2661

[400] VAZ, Bruna; ZOMBARDI, José Lucas; GUEIROS, Pedro. **O caso "Google x Marielle Franco" e a quebra do sigilo telemático genérica.** Consultor jurídico. 26/10/2023. Disponível em: https://www.conjur.com.br/2023-out-26/opiniao-google-marielle-franco-quebra-sigilo-telematico-generica/#:~:text=Para%20melhor%20compreens%C3%A3o%2C%20a%20quebra,de%20crime%2C%20mediante%20autoriza%C3%A7%C3%A3o%20judicial. 4 p.

[401] CCDCOE. **EU Data Retention Directive Union.** Disponível em: https://ccdcoe.org/incyder-articles/eu-data-retention-directive-invalid/#footnote_1_2661

[402] COURT OF JUSTICE OF THE EUROPEAN UNION. **The Court of Justice declares the Data Retention Directive to be invalid**. Luxembourg, 08/04/2014. Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Outra questão de fundamental importância para a implantação de *smart city* é o combate à discriminação no ambiente tecnológico. Esse assunto tem sido debatido em diversos países, especialmente para a regulamentação da inteligência artificial.

No Brasil, juristas defendem que o uso de programas inteligentes no setor público só pode ser aprovado após um estudo do impacto social do programa. O propósito é evitar a discriminação de grupos vulneráveis como minorais raciais, menores, idosos e pessoais com deficiência[403].

Esta ideia surgiu após os problemas ocorridos no sistema algorítmico de distribuição do auxílio emergencial que decidia quem teria ou não direito ao benefício. As pessoas que recebiam a negativa da concessão do auxílio não tinham como recorrer administrativamente da decisão algorítmica e, por conta disso, buscavam o meio judicial[404].

Em resumo, os algoritmos representam uma sequência de ações que possuem uma finalidade específica, seja para executar uma tarefa ou resolver um problema[405]. O objetivo dos algoritmos é, especialmente, solucionar problemas e auxiliar na tomada de decisão. Também há casos em que os algoritmos não são capazes de fornecer uma resposta precisa e, portanto, fazem previsões com base em probabilidades. [406]

Esses algoritmos agem de acordo com os dados que os alimentam. Quanto maior é a quantidade e a qualidade dos dados fornecidos, maior a chance de o resultado fornecido pelo sistema ser útil.

Com efeito, o desenvolvimento de tecnologias de *Big Data* possibilitou a elaboração de previsões baseadas em um grande número de informações, sobre qualquer tipo de assunto, inclusive relacionado ao comportamento individual. Este contexto ainda se torna mais

---

[403]FRAGOSO, Roberto. **Comissão de juristas debate discriminação tecnológica por inteligência artificial.** SENADO FEDERAL 12/05/2022 disponível em: https://www12.senado.leg.br/radio/1/noticia/2022/05/12/comissao-de-juristas-da-inteligencia-artificial-debate-discriminacao-tecnologica

[404] FRAGOSO, Roberto. **Comissão de juristas debate discriminação tecnológica por inteligência artificial**. SENADO FEDERAL 12/05/2022 disponível em: https://www12.senado.leg.br/radio/1/noticia/2022/05/12/comissao-de-juristas-da-inteligencia-artificial-debate-discriminacao-tecnologica

[405] SILVA, Maria Fernanda; OLIVEIRA, Cristina Godoy Bernardo de. **O impacto social causado pelo uso de algoritmos discriminatórios e a superveniência da LGPD.** Migalhas. 04/11/2022 Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/376497/o-impacto-social-causado-pelo-uso-de-algoritmos-discriminatorios

[406] MANTUSO, Marcela; MENDES, Laura Schertel. **Discriminação algorítmica: Conceito, fundamento legal e Tipologia.** Proteção de dados e inteligência artificial: Perspectivas éticas e regulatórias. Porto Alegre. Dezembro de 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019 4 p.

complexo com a inserção da Inteligência Artificial, que auxilia o desenvolvimento de máquinas que utilizam técnicas de *machine learning*. [407].

A ascensão das técnicas de aprendizado de máquina, como o *machine learning*, trouxe problemas relacionados à obscuridade de processos decisórios. Ademais, há casos em que os próprios desenvolvedores e programadores não sabem como o algoritmo chegou a um determinado resultado, muitas vezes porque o seu processo de aprendizagem não é supervisionado[408].

Um exemplo famoso ocorreu nos Estados Unidos, no processo *State v. Loomis*[409], que envolveu um software de avaliação de riscos chamado *Correctional Offender Management Profiling for Alternative Sanction*s (COMPAS) para avaliar o risco de reincidência de infratores. Este sistema calcula a probabilidade de um indivíduo com antecedentes criminais em cometer um novo crime.

No caso, Eric Looomis recebeu cinco acusações criminais relacionadas a um tiroteio em *La Croose*. Loomis se declarou culpado de duas dessas acusações, quais sejam, a tentativa de fuga e a operação de veículo motorizado sem o consentimento do proprietário.

Durante a confecção da sentença, foi utilizada a avaliação de risco COMPAS para estimar o risco de Loomis de cometer novos crimes. Uma vez que a metodologia do COMPAS é um segredo comercial, apenas a estimativa do risco de reincidência de Loomis foi comunicada ao tribunal. Com base nessa avaliação e em outros argumentos, Loomis foi condenado a seis anos de prisão[410].

A defesa de Loomis recorreu da decisão, argumentando que houve violação ao direito do devido processo legal do réu, uma vez que a metodologia usada pelo COMPAS era um segredo comercial e ninguém sabia o motivo do resultado. Alegou-se ainda que a avaliação do COMPAS considerou a característica de gênero e, portanto, a sentença era inconstitucional.

---

[407] MANTUSO, Marcela; MENDES, Laura Schertel. **Discriminação algorítmica: Conceito, fundamento legal e Tipologia.** Proteção de dados e inteligência artificial: Perspectivas éticas e regulatórias. Porto Alegre. Dezembro de 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019 5 p.

[408] SILVA, Maria Fernanda; OLIVEIRA, Cristina Godoy Bernardo de. **O impacto social causado pelo uso de algoritmos discriminatórios e a superveniência da LGPD**. Migalhas. 04/11/2022 Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/376497/o-impacto-social-causado-pelo-uso-de-algoritmos-discriminatorios

[409] HAVARD LAW REVIEW. **State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessment in Sentences**. 2016. Disponível em: https://harvardlawreview.org/print/vol-130/state-v-loomis/

[410] HAVARD LAW REVIEW. **State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessment in Sentences.** 2016. Disponível em: https://harvardlawreview.org/print/vol-130/state-v-loomis/

A Suprema Corte de Wisconsin manteve a decisão de primeira instância, alegando que o uso de tecnologia algorítmica por um tribunal para avaliar o risco de reincidência não violou o direito ao devido processo do réu. Também serviram de base da decisão da Suprema Corte o fato de a sentença não ser baseada somente na avaliação do COMPAS, que este sistema apenas utiliza dados publicamente disponíveis e dados fornecidos pelo arguido e que Loomis poderia ter explicado qualquer informação utilizada no relatório.

Entende-se que a influência do COMPAS na condenação de primeiro grau, por si só, já viola o devido processo legal, pois são desconhecidas as circunstâncias avaliadoras consideradas pelo sistema eletrônico e o peso de cada circunstância sobre o resultado. A falta de transparência do sistema impossibilitou o poder de argumentação da defesa do réu, além de colocar em dúvida se houve alguma informação de viés discriminatório considerado na avaliação algorítmica.

A discriminação algorítmica também ocorre em setores privados, a exemplo do uso de algoritmos para selecionar candidatos a vagas de emprego. Há muitas empresas que abandonaram os processos seletivos tradicionais, adotando softwares que realizam todo o processo de recrutamento de pessoas por meio de um perfil previamente traçado pelo algoritmo.

No entanto, se uma pessoa não estiver dentro dos padrões do software entendidos como ideais para o emprego, ela será excluída dos processos de recrutamento. Este é o caso de Kyle Behm, que, por ter sido diagnosticado com transtorno bipolar, não foi selecionado para diversas vagas de emprego em diferentes empresas[411].

Outro caso que gerou repercussão internacional foi a acusação de discriminação contra mulheres no sistema de pontuação do *Apple Card*. Em resumo, a empresa *Apple* lançou um cartão de crédito em parceria com a *Wall Street Goldman Sachs*, como forma de inserir seus produtos na indústria financeira[412].

Todavia, surgiu um problema nos algoritmos no sistema de crédito do cartão, do qual oferecia maiores valores de créditos para homens do que para mulheres. O algoritmo de IA apresentou um viés discriminatório de gênero porque foi treinado com base em dados enviesados[413].

---

[411] O NEIL, Cathy. **Personality Tests Are Failing American Workers**. Bloomberg. 18/01/2018. Disponível em: https://www.bloomberg.com/view/articles/2018-01-18/personality-tests-are-failing-american-workers

[412] BAMBROUGH, Billy. **Apple Card é acusado de discriminação contra mulheres.** Forbes. 11/11/2019 Disponível em: https://forbes.com.br/forbes-mulher/2019/11/apple-card-e-acusado-de-discriminacao-contra-mulheres/

[413] SILVA, Maria Fernanda; OLIVEIRA, Cristina Godoy Bernardo de. **O impacto social causado pelo uso de algoritmos discriminatórios e a superveniência da LGPD.** Migalhas. 04/11/2022 Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/376497/o-impacto-social-causado-pelo-uso-de-algoritmos-discriminatorios

Além dos casos de monitoramento eletrônico em massa e discriminação analisados, existem vários outros que devem ser estudados, principalmente por juristas e desenvolvedores de tecnologia em ambientes urbanos, para que não ocorra o mesmo nas cidades inteligentes[414].

Os casos estudados neste trabalho mostram um cenário preocupante na implantação de *smart city,* que tem uma capacidade exponencial de violar os direitos do cidadão aqui analisados. O sucesso da cidade inteligente depende da criação de um ambiente seguro, tanto para os cidadãos como para os desenvolvedores de tecnologia.

CAPÍTULO III: BUSCANDO SOLUÇÕES PARA A PROTEÇÃO DE DADOS PESSOAIS EM SMART *CITIES*

Este capítulo traz algumas medidas governamentais estrangeiras, criativas e atuais, que buscam minimizar os problemas relativos à proteção de dados pessoais no contexto digital, alguns deles identificados no capítulo anterior. Essas medidas estão diretamente ligadas à implantação de *smart city* no ambiente tecnológico urbano, uma vez que operam sobre os produtos e serviços de TIC, como *cloud,* dispositivos habilitados em IoT e *big data.*

Cada item deste capítulo é o resultado de pesquisas realizadas em materiais estrangeiros dos países, regiões e cidades identificados ao longo deste trabalho e considerados avançados na implantação de tecnologia *smart city.* Entre os documentos estrangeiros analisados estão legislações, programa municipal e regional de implantação de *smart city* em ambiente urbano, guias e ferramentas de proteção de dados.

3.1. *Privacy By Design*

O termo *Privacy by Design* é tratado no artigo 25 do GDPR, e entendido como *a proteção de dados através da concepção da tecnologia*[415]. As primeiras impressões sobre a

[414]Apenas como exemplos, citam-se o *cambridge analytica*, empresa que utilizava dados de usuários do Facebook para influenciar a opinião dos eleitores em vários países. Disponível em: https://www.bbc.com/portuguese/internacional-43461751 e os casos de racismo em sistemas de reconhecimento fácil tratados no documentário *Cooded Bias* da Netflix. Disponível em: https://www.netflix.com/title/81328723

[415] "The term "Privacy by Design" means nothing more than "data protection through technology design." Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created. Nevertheless, there is still uncertainty about what "Privacy by Design" means, and how one can implement it". INTERSOFT CONSULTING. **GDPR. Privacy By Design.** Disponível em: https://gdpr-info.eu/issues/privacy-by-design/#:~:text=GDPR%20Privacy%20by%20Design&text=The%20term%20%E2%80%9CPrivacy%20by%20Design,in%20the%20technology%20when%20created.

privacidade desde a concepção foram expressas na década de 1970, mas foram incorporadas na legislação europeia na diretiva de proteção de dados RL 95/46/CE[416]

O *Privacy by Design* consiste em sete princípios sobre a proteção da privacidade que devem ser observados desde a criação de um produto ou de um serviço. Apesar de não ser uma novidade, o seu conceito é atual, e serve para combater problemas sistémicos de tecnologias de comunicação e de sistemas de dados em rede em longa escala[417].

O *Proative not Reactive; Preventative not Remedial* é o primeiro princípio do *Privacy By Design* e se caracteriza por medidas preventivas que visam evitar a ocorrência de infrações a privacidade. Sua natureza está pautada na valoração dos benefícios da proteção à privacidade e na adoção de medidas práticas protetivas superiores aos padrões exigidos por leis e regulamentos.

Outro princípio é o *Privacy by Default,* que adota a privacidade como padrão de qualquer produto ou serviço, tornando-a um componente do sistema ou da prática comercial. Desse modo, quando o produto ou serviço chega às mãos do consumidor final, ele já se encontra em um grau elevado de proteção à privacidade, não necessitando de nenhuma ação para elevar o nível de proteção.

Assim, para tornar a privacidade um padrão do serviço ou produto, é necessário informar a finalidade do tratamento de dados ao titular antes ou no momento da coleta. Ademais, a coleta de dados pessoais deve ser mínima e limitada à finalidade informada.

---

[416]INTERSOFT CONSULTING. **GDPR. Privacy By Design.** Disponível em: https://gdpr-info.eu/issues/privacy-by-design/#:~:text=GDPR%20Privacy%20by%20Design&text=The%20term%20%E2%80%9CPrivacy%20by%20Design,in%20the%20technology%20when%20created.

[417] "Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS Plus — taking a positive-sum (full functionality) approach, not zero-sum. That's the "Plus" in PETS Plus: positive-sum, not the either/or of zero-sum (a false dichotomy). Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure. Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data. The objectives of Privacy by Design — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles." CAVOUKIAN, ANN. **Privacy By Design, the 7 Foundational Principles.** Ontario, Canada 2009. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pd>

Por fim, as informações pessoais devem estar em posse dos controladores apenas durante o período necessário para alcançar a finalidade pretendida e informada ao titular. Após este prazo, os dados pessoais devem ser destruídos através de um meio seguro.

O terceiro princípio é o *Privacy Embedded into design* e preconiza que a privacidade deve ser incorporada na arquitetura dos sistemas tecnológicos e nas práticas negociais. A consequência disso é a privacidade como parte integrante do sistema sem que ela diminua a sua funcionalidade.

O *Full Functionalty – Positive- Sum, not Zero-sun* é o quarto princípio do *Privacy by Design* e defende a ideia de que todos os interesses são legítimos e, por isso, devem ser observados durante o desenvolvimento do produto ou serviço. Este princípio objetiva evitar os conflitos entre a privacidade e outras prerrogativas, como a segurança, buscando um caminho que contemple todos os fatores.

O *End-to-End Security – Lifecycle Protection* é entendido por preconizar a segurança dos dados pessoais durante todo o seu ciclo, desde antes da coleta até a sua destruição. Assim, o controlador adota medidas de segurança em todas as fases em que ele tem relação com os dados pessoais.

Os padrões de segurança aplicados devem garantir a confidencialidade, a integridade e a disponibilidade dos dados pessoais durante todo o ciclo de tratamento. Para que isso ocorra, devem ser adotados métodos de segurança de destruição de dados segura, criptografia robusta e rigorosos controles de acesso e registro.

Outro princípio é o *Visibility and Transparency,* que busca a transparência do tratamento dos dados pessoais bem como o seu fácil acesso, tanto para usuários como para fornecedores. A sua proposta é garantir que as operações com dados pessoais possam ser verificadas pelos interessados.

A observância desse princípio é fundamental para a implantação de tecnologia *smart city* em ambientes urbanos, pois fortalece a confiança da população sobre as operações envolvendo dados pessoais. Na prática, o agente deve demonstrar que adotou medidas eficazes para o cumprimento das imposições do sistema de proteção de dados pessoais *(accountability)*.

Também é importante que o agente disponibilize as suas políticas e práticas referentes ao gerenciamento de informações pessoais. Ainda, criam-se meios simples de comunicação entre o agente e os titulares para que estes possam exercer os seus direitos como de retificação de dados incorretos e de portabilidade dos dados.

O sétimo e último princípio é o *Respect for User Privacy,* e determina que os interesses do titular dos dados pessoais devem se sobrepor a qualquer outro. Desse modo, a opção de

desenvolvimento do produto e do serviço mais adequada é aquela que melhor atende às necessidades e interesses do usuário.

Como exemplos cita os padrões robustos de privacidade, as opções mais práticas de utilização do produto ou serviço bem como a adoção da forma mais simples de visualização. Esse princípio se estende para qualquer tecnologia, que deve ter como objetivo central o atendimento às necessidades do ser humano, indo de encontro com os objetivos do Direito Urbanístico.

A época da criação do *privacy by design*, já havia a desconfiança de que as leis e os regulamentos não poderiam proteger a privacidade dos usuários no ambiente tecnológico. Nos dias atuais, essa desconfiança persiste e pode ter aumentado por conta das limitações técnicas das tecnologias de TIC descritas no capítulo anterior.

Desse modo, as regiões e as cidades mais avançadas em implantação de tecnologia inteligente estão exigindo a criação de produtos e serviços tecnológicos baseados no *privacy by design.* Um exemplo é a *Public London Charter* (PLC), documento orientativo do *London Plan Guidance* (LPG), criado pela prefeitura de Londres para estabelecer direitos e responsabilidades de pessoas dentro do novo espaço público da cidade e que será analisado em tópico posterior[418].

Outro exemplo é a *European Union Agency for Cibersecurity* – ENISA, Agência da União Europeia dedicada a promover um elevado nível comum de cibersegurança entre os países membros[419]. A ENISA propõe a aplicação do *privacy by design* no desenvolvimento e na implementação de serviços de saúde que utilizam a tecnologia *cloud.*

Em seu relatório específico sobre *Cloud Security for Healthcare Services,* a ENISA relata a dificuldade de compreensão do prestador de serviço de saúde sobre a importância do *privacy by design* para o seu produto ou serviço baseado em *Cloud.* [420]. Algumas das exigências da ENISA são a possibilidade de monitoramento do tratamento de dados pessoais pelo seu titular e o aprimoramento de medidas de segurança como controle de divulgação de estatísticas e o desenvolvimento de comunicações privadas seguras.

Por fim, também é adotado o *Privacy By Design* nas orientações do *Office of the Australian Information Commisssioner* (OAIC) para a criação e o desenvolvimento de produtos

[418]MAYOR OF LONDON. **London Plan Guidance.** 2021. Disponível em: https://www.london.gov.uk/publications/public-london-charter
[419]EUROPEAN UNION AGENCY FOR CIBERSECURITY. Disponível em: https://www.enisa.europa.eu/
[420]EUROPEAN UNION AGENCY FOR CIBERSECURITY. **Cloud Security for Healthcare Services**. 18/01/2021.Disponível em: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services 18 p.

e serviços de organizações e de agências governamentais australianas[421]. Segundo a OAIC, antes de aplicar o *Privacy By Design,* é necessário compreender os impactos que o produto ou o serviço de tecnologia pode causar sobre os direitos de privacidade e de proteção de dados pessoais do usuário.

Dessa forma, o OAIC orienta que às organizações devem desenvolver, antes da comercialização do produto ou serviço tecnológico, o *Privacy Impact Assessment*. Este documento realiza uma avaliação sistemática do produto ou serviço, investigando os impactos sobre a privacidade dos indivíduos e formulando recomendações para minimizar ou eliminar os impactos identificados.

3.2. *London Plan Guidance* (LPG)

As estratégias da autoridade municipal britânica para a implantação segura de tecnologia em ambientes urbanos são fornecidas pelo *London Plan Guidance*[422]. Publicado no ano de 2021, o LPG foi formalmente adotado pelo prefeito de Londres, Sadiq Khan[423].

Este plano municipal possui uma série de orientações, códigos, e cronogramas voltados para a implantação de tecnologia na cidade de Londres. O LPG é estruturado por assuntos, tais como, habitação, infraestrutura social, transporte, infraestrutura verde e design.

Dentre os seus documentos, há a *Public London Charter* (PLC), carta direcionada ao desenvolvimento tecnológico em novos espaços públicos[424]. A PLC é imposta pela Política D8 do Plano de Londres[425] , e tem o objetivo de garantir que os novos espaços públicos sejam seguros, acessíveis e inclusivos.

Durante a confecção da PLC, foi realizado a *Equality Impact Assessment*, uma avaliação de impacto que trata sobre questões de igualdade. Os objetivos traçados para o setor público

---

[421]AUSTRALIAN GOVERNMENT. **Office of the Australian Information Commissioner. Privacy By Design** Disponível em: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/privacy-by-design

[422]MAYOR OF LONDON. **London Plan Guidance.** Disponível em: https://www.london.gov.uk/programmes-strategies/planning/implementing-london-plan/london-plan-guidance

[423] MAYOR OF LONDON. **MD2861 London Plan Guidance.** 16/09/2021. Disponível em: https://www.london.gov.uk/decisions/md2861-london-plan-guidance

[424]MAYOR OF LONDON. **Public London Charter**. Disponível em: https://www.london.gov.uk/programmes-strategies/planning/implementing-london-plan/london-plan-guidance/public-london-charter

[425]"H - ensure appropriate management and maintenance arrangements are in place for the public realm, which maximize public access and minimize rules governing the space to those required for its safe management in accordance with the Public London Charter" MAYOR OF LONDON. **The London Plan**. Disponível em: https://www.london.gov.uk/sites/default/files/the_london_plan_2021.pdf 135 p.

foram eliminar a discriminação e o assédio, além de promover a igualdade de oportunidades e as boas relações entre grupos de pessoas com características distintas.[426]

A PLC possui oito princípios que impõem uma série de obrigações aos proprietários, aos gestores de empreendimento e às autoridades de planejamento dos novos espaços públicos. Aqueles que pretendem desenvolver um novo espaço público em Londres deverão provar, através de um plano de gestão, como os requisitos da PLC serão cumpridos, e assinar um contrato concordando com a implementação dessas medidas[427].

Um dos princípios da PLC é o *Privacy and Data,* que protege os direitos à privacidade e à proteção de dados pessoais do cidadão na implantação de tecnologia inteligente em espaço público. A Carta impõe aos desenvolvedores de tecnologias a obrigação de realizar testes, criados pelo *Information Comissioner's Ofice* (ICO) do Reino Unido, dos novos produtos e serviços. Caso o produto ou serviço não atenda aos requisitos determinados pelo ICO, será proibida a sua utilização nos espaços públicos de Londres[428].

O *Privacy and Data* descrito na Carta reconhece os vários benefícios trazidos pela tecnologia aos serviços públicos. Todavia, pondera sobre aos riscos aos direitos do cidadão no uso da tecnologia no ambiente urbano.

Por conta disso, a *Public London Charter* orienta a utilização do *privacy by design*, que garante a proteção de dados pessoais e a conformidade com a privacidade desde a concepção do produto ou serviço. Ainda, a PLC propõe ao desenvolvedor que incentive a participação dos usuários durante o desenvolvimento do seu produto ou serviço inovador[429].

Para o caso específico de tecnologia inteligente que utiliza CCTV o PLC impõe o cumprimento do *Surveillance Camera Commissioner's Code of Pratice*[430], além da observância da UK GDPR e da *Data Protection Act* de 2018. A *Public London Charter* destaca o risco de

---

426 MAYOR OF LONDON, **Equality Impact Assessment (EqIA) for London Plan Guidance**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.london.gov.uk/sites/default/files/public_london_charter_lpg_eqia.pdf 1 p.

427MAYOR OF LONDON. **Public London Charter**. Disponível em: https://www.london.gov.uk/programmes-strategies/planning/implementing-london-plan/london-plan-guidance/public-london-charter 4 p.

428MAYOR OF LONDON. **Public London Charter**. Disponível em: https://www.london.gov.uk/programmes-strategies/planning/implementing-london-plan/london-plan-guidance/public-london-charter 14 p.

429 "4.6.5 People need to be able to trust the way personal data is used so that the technologies can provide genuine and inclusive benefits. The Data Protection Act (2018) closely regulates the collection and use of personal data. In line with this, landowners and managers of public spaces should be clear about why they are collecting any personal data and take a ***'privacy by design'*** approach, which ensures data protection and privacy compliance from the beginning. Users should be involved in this process where appropriate." INFORMATION COMISSIONER'S OFICE. **Public London Charter.** Disponível em: https://www.london.gov.uk/publications/public-london-charter 14 p.

430UNITED KINGDOM. **Guidance Surveillance Camera Commissioner's Code of Pratice.** Disponível em: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

violação ao princípio da não discriminação na utilização de dados biométricos e pessoais recolhidos automaticamente em locais públicos para operações de tratamento de dados pessoais de reconhecimento facial.

Por fim, o *Privacy and Data* determina que as avaliações de impacto e proteção de dados pessoais dos gestores, proprietários e autoridades dos novos espaços públicos sejam compartilhadas com a prefeitura para que sejam publicadas no *London Datastore*. Essa medida visa promover a conformidade, as boas práticas e a transparência.

Por falar nisso, a *Transparency* é outro princípio da PLC e impõe aos responsáveis a publicação dos direitos e regras do espaço público. Devem ser fornecidos, além da *Public London Charter*, as regras específicas do local e os dados sobre o gestor daquele espaço público.

Essas informações devem ser claras e acessíveis a todos, tanto através do meio online como disponibilizadas no próprio local. O fornecimento das informações auxilia na supervisão da conformidade do espaço público com os princípios constantes na PLC.

A *Public London Charter* determina que as regras específicas do novo espaço público devem ser desenvolvidas mediante consulta da comunidade em geral interessada. Mais uma vez, identifica a importância do envolvimento da população para a inserção de tecnologia que utiliza dados pessoais no ambiente urbano.

O *London Plan Guidance* é um bom exemplo de documento orientativo para a implantação de *smart city* no ambiente urbano. Muitas de suas estratégias podem ser adotadas no Brasil e, portanto, merece um estudo específico.

3.3. *Children's Code - United Kingdom*

O *Children 's Code, ou Age Apropriate Design Code,* são padrões direcionados aos serviços online que servem para garantir o cumprimento das obrigações, constantes na UK GDPR, relativas à proteção dos menores de idade no ambiente digital. Apesar de não ser um documento criado especificamente para *smart city,* ele deve ser observado pelas organizações que nele se enquadram.

Este código se aplica a todo serviço da sociedade de informação (SSI) que possa ser prestado para crianças, á distancia, por meio eletrônico, mediante remuneração e por solicitação individual do destinatário do serviço[431]. Consideram-se serviços da sociedade da informação,

[431]INFORMATION COMMISSIONER'S OFFICE. **Introduction to the Childre's code**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/

entre outros, os aplicativos, os jogos online, os brinquedos que possuam dispositivos conectados, as plataformas de mídia social, os serviços de notícias, os mercados online, os serviços de streaming de conteúdo e motores de busca.

O *Children 's Code* se aplica a todas as empresas, sejam elas sediadas ou não no Reino Unido, que processam dados pessoais de menores que estão em UK. O documento impõe quinze padrões gerais[432] de boa prática que devem ser cumpridos pelo fornecedor de SSI, a depender da situação em que o seu serviço se encaixa. Para o caso de tecnologias educacionais ou *edtechs*, o ICO desenvolveu orientações específicas.[433]

O *best interests of the child,*é um padrão que deve ser considerado durante a criação do serviço online, e determina o melhor interesse da criança como fator primordial no desenvolvimento do produto ou serviço tecnológico.

O *data protection impact assessments* (DPIA) – em português, avaliação de impacto e proteção de dados – é o segundo padrão do *Children's Code* e é um documento que tem como finalidades avaliar e mitigar os riscos contra os direitos e liberdades das crianças durante o processamento dos seus dados. Neste caso, o DPIA deve levar em consideração as capacidades e necessidades de desenvolvimento de cada faixa etária.

O terceiro padrão é o *age appropriate application,* que impõe a adoção de sistemas capazes de reconhecer a idade do usuário e de garantir a aplicação eficaz dos padrões do código para o público infantil. Caso não seja possível determinar a idade para o processamento dos dados, o prestador de SSI deve aplicar os padrões do *Childen's Code* a todos os seus usuários.

O quarto padrão é o *transparency* que obriga o fornecimento de informações de privacidade para a comunidade, tais como, as políticas, a ampla divulgação desses padrões e explicações adicionais específicas do serviço sobre o uso dos dados pessoais. A linguagem utilizada deve ser clara e adequada à idade da criança que utiliza o serviço.

O *detrimental use of data* é um padrão que impõe a proibição sobre as formas de uso de dados pessoais de crianças que são comprovadamente prejudiciais ao bem-estar do menor. Esta proibição se estende a formas que estão em desencontro com códigos de prática da indústria ou qualquer outra disposição regulamentar ou recomendação do governo.

---

[432]INFORMATION COMMISSIONER'S OFFICE. **Code standards**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/

[433] INFORMATION COMMISSIONER'S OFFICE. **The Children's code and education Technologies (edtech).** Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/

O sexto padrão é o *policies and community standards,* que determina ao prestador de SSI a criação e a publicação sempre atualizadas dos seus termos, políticas de conteúdo e de privacidade, restrição de idade e regras de comportamento.

Já o *default settings* consiste na obrigação de manter as configurações dos serviços online num padrão de alta privacidade. O desenvolvedor de SSI pode não cumprir este requisito caso comprove que uma configuração padrão diferente irá atender aos melhores interesses da criança.

O oitavo padrão é o *data minimisation* que determina aos desenvolvedores o respeito a quantidade mínima de coleta e retenção de dados pessoais dos menores, suficiente para fornecer o serviço. A criança deve estar ativa e conscientemente envolvida na coleta de seus dados.

O *data sharing* é uma regra que proíbe a divulgação de dados pessoais de crianças aos prestadores de serviços online. A exceção desta regra pode ocorrer se for comprovado o melhor interesses do menor.

O décimo padrão é o *geolocation* que proíbe a opção ativa de geolocalização por padrão no SSI, a menos que seja comprovado o melhor interesse da criança. O SSI deve fornecer um sinal, facilmente perceptível à criança, capaz de mostrar que o rastreamento de localização está ativo. A opção que confere ao terceiro a permissão de visualizar a localização da criança deve ser desativada no momento do encerramento do serviço.

O *parental controls* é o décimo primeiro padrão, destinado a serviços online que permite o monitoramento dos pais ou responsável sobre as atividades online de seu filho ou o rastreamento da sua localização. Nessa hipótese, o serviço deve fornecer à criança informações, com linguagem própria à sua idade, sobre o controle parental, além de um sinal, facilmente visível para o menor, nas hipóteses de monitoramento da criança.

O *profiling* consiste em desativar a configuração de criação de perfil por padrão. Essa criação só é permitida caso o SSI possua a capacidade de fornecer medidas adequadas e eficazes de proteção à criança contra conteúdos prejudiciais à sua saúde e ao seu bem-estar.

O décimo terceiro padrão é o *nudge techniques* que proíbe o uso de técnicas de persuasão para incentivar crianças a fornecer dados pessoais desnecessários ou enfraquecer ou desativar suas proteções de privacidade.

O *connected toys and services* é destinado ao fornecedor de brinquedo ou dispositivo conectado. Este requisito determina a criação de ferramentas eficazes que sejam capazes de adaptar o produto tecnológico aos padrões do *Children s Code.*

Por fim, o último padrão é o *online tools*, que impõe a criação de ferramentas de ajuda online à criança usuária. Essas ferramentas devem ser de fácil acesso e permitir que a criança exerça o seu direito de comunicação, realizando reclamações e esclarecendo dúvidas.

Para potencializar a implantação do *Children s Code*, o ICO disponibiliza orientações e fornece modelos de documentos como *The ICO' s Best interests of the child self- assessment*. Este documento confere ao prestador de SSI ferramentas, modelos e orientações para garantir o cumprimento do padrão sobre o melhor interesse da criança[434].

Também é disponibilizado pelo ICO o *Children s Code Self-Assessment Risk Toll,* voltado para organizações, de médio e grande porte, públicas, privadas e do terceiro setor. Esse documento consiste em uma autoavaliação de risco que verifica a garantia da segurança e da proteção da privacidade das crianças conforme o UK GDPR e o *Children s Code[435]*.

Outra iniciativa interessante para a *smart city* é o *small bussiness wed hub[436],* um espaço digital destinado às empresas de pequeno porte. Nele, há orientações por assunto, um suporte do ICO exclusivo a estas empresas e guias práticos para o iniciante de proteção de dados[437].

Dentre os guias práticos, destaca o *begginner's guide to data protection*, que oferece um passo-a-passo simples e objetivo para as empresas de pequeno porte. Esse guia promove a execução de importantes medidas que asseguram a aplicação de algumas regras principais da lei de proteção de dados pessoais britânica.

Outro guia prático que merece menção é o *How to write a privacy notice and what goes in it[438],* que orienta sobre a confecção da política de privacidade para comerciantes individuais, pequenas e médias empresas. Este guia sugere que a política de privacidade deve ser curta e simples, especialmente se houver o tratamento de dados pessoais de crianças.

Por fim cita a orientação específica para pequenas organizações que desejam utilizar câmeras CCTV ou tecnologia semelhante[439]. São etapas básicas preparatórias, ou seja, medidas

---

[434] INFORMATION COMMISSIONER'S OFFICE. **Best interests of the child self- assessment**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/

[435]INFORMATION COMMISSIONER'S OFFICE. **Children s Code Self-Assessment Risk Toll** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/children-s-code-self-assessment-risk-tool/

[436]NFORMATION COMMISSIONER'S OFFICE. **Find the right resource**. Disponível em: https://ico.org.uk/for-organisations/advice-for-small-organisations/find-the-right-resource/

[437]INFORMATION COMMISSIONER'S OFFICE **Your beginner's guide to data protection.** Disponível em: https://ico.org.uk/for-organisations/advice-for-small-organisations/your-beginner-s-guide-to-data-protection/

[438]INFORMATION COMMISSIONER'S OFFICE **How to write a privacy notice and what goes in it.** Disponível em: https://ico.org.uk/for-organisations/advice-for-small-organisations/how-to-write-a-privacy-notice-and-what-goes-in-it/

[439]INFORMATION COMMISSIONER'S OFFICE **Instaling CCTV? Things you need to do first.** *Disponível em:* https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/installing-cctv-things-you-need-to-do-first/

anteriores à instalação da tecnologia para a promoção da proteção dos dados pessoais e da privacidade.

3.4. *Synchronicity – European Union*

O *Synchronicity* foi a primeira tentativa de criação de um mercado único de cidade digital habilitado em IoT na União Europeia e foi testado em onze cidades, sendo oito delas localizadas na Europa e três em outras regiões do mundo[440]. Este era um dos projetos do *Horizon 2020*, um programa financiado pelos países membros da União Europeia que teve como objetivo promover a inovação na UE[441].

O principal objetivo do *Synchronicity* era desenvolver um ecossistema integrador de *smart city* em IoT, que promovesse a livre competição entre os fornecedores de produtos e serviços tecnológicos. A plataforma digital utilizada para o mercado em IoT seria fornecida por uma entidade neutra e observaria os regulamentos de governança e proteção de dados da UE[442].

O *Synchronicity* propôs a criação de uma arquitetura de referência para o mercado urbano de IoT, com pontos de interoperabilidade, interfaces e modelo de dados para diferentes setores, reduzindo as barreiras de participação para este mercado. A *Guideline* do projeto estabeleceu os atributos desejáveis de um mercado único digital para serviços urbanos baseados em IoT[443].

A estratégia adotada pelo projeto foi a de permitir a participação de componentes externos, tais como, empresas de TIC desenvolvedoras de produtos ou serviços em IoT, potenciais consumidores e cidades interessadas. Desse modo, o *Synchronicity* contou com o *Open & Agile Smart Cities & Communities,* uma organização sem fins lucrativos que possui mais de 150 cidades membros espalhadas pelo mundo, e tem como objetivo criar um mercado global de serviços digitais para cidades e comunidades.[444]

---

[440]EUROPEAN COMISSION. **Synchronicity: Delivering an IoT enabled Digital Single Market for Europe and Beyond.** Disponível em: https://cordis.europa.eu/project/id/732240

[441]EUROPEAN COMISSION: **Horizon 2020. Details of the UE funding programme which ended in 2020 and links to futher information** Disponível em: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en

[442] GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. **Guidelines for SynchroniCity architecture.** disponível em: https://cordis.europa.eu/project/id/732240/results 13 p.

[443] GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. **Guidelines for SynchroniCity architecture**. disponível em: https://cordis.europa.eu/project/id/732240/results 12 p.

[444]OPEN & AGILE SMART CITIES & COMMUNITIES. Disponível em: https://oascities.org/

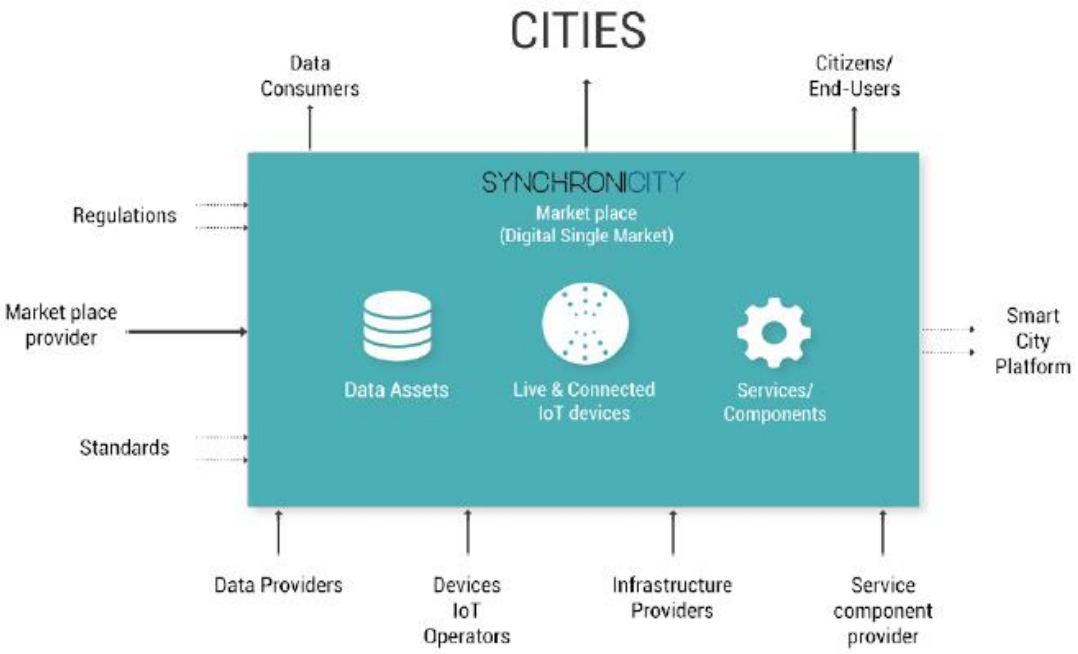

Figura 4: Interação entre os *stakeholders* no mercado único digital *SynchroniCity*[445].

Para adequar o *Synchronicity* ao GDPR, foi desenvolvida uma estratégia de proteção de dados com três alicerces: 1) O duplo DPO; 2) A avaliação de impacto de proteção de dados pessoais para *smart city* e; 3) Um aplicativo de privacidade.

Foi considerada controladora de dados cada uma das onze cidades onde a arquitetura do *Synchronicity* foi testada. Desse modo, cada cidade tinha autonomia para determinar quais seriam as suas operações com dados pessoais e como os tratamentos seriam processados[446].

Ficou acordado entre os controladores do projeto que cada cidade teria a obrigação de nomear um DPO municipal. Algumas de suas funções e responsabilidades eram: monitorar a conformidade das operações de dados pessoais dos demais controladores da sua cidade com o GDPR, a exemplo de universidades, desenvolvedores de aplicativos e empresas de IoT; formular um relatório com uma visão geral sobre a coleta e o processamento de dados pessoais da cidade e; realizar a avaliação de impacto e proteção de dados (AIPD).

Ademais, os DPO's municipais teriam que reportar o seu serviço para o coordenador dos DPO's, que era o DPO da *Synchronicity*. Assim foi criado o termo duplo DPO, que nada mais é que um organograma formado por vários DPO's municipais em sua base e um coordenador dos DPO's na ponta da pequena pirâmide organizacional.

---

[445] GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. **Guidelines for SynchroniCity architecture**. disponível em: https://cordis.europa.eu/project/id/732240/results 13 p.
[446] ZIEGLER, Sébastien. **Internet of Things Security and Data Protection.** Springer. 2019 158 p.

Entre outras funções, o coordenador dos DPO's supervisionava e orientava o DPO's municipais. Também, foi criado um *Data Protection Commitee* que era formado por todos os DPO's municipais do projeto, sob a presidência do coordenador dos DPO's, e tinha como objetivos: definir e atualizar a política de proteção de dados do *Synchronicity,* resolver os problemas que surgiam durante a execução do projeto e atualizar a população com novas informações acerca da proteção de dados pessoais.

A segunda base da proteção de dados pessoais do *Synchronicity* era a avaliação de impacto de proteção de dados (AIPD) para *smart city* que foi realizada antes e durante à execução do projeto, por cada uma das cidades participantes. Esta era uma avaliação específica, projetada e adaptada para abordar as necessidades e os potenciais riscos relacionados à implantação de IoT no ambiente urbano[447].

A avaliação teve como base primordial a abordagem do *privacy by design* na implantação de IoT nas cidades, orientando os controladores de dados neste sentido. Ademais, a AIPD da cidade inteligente era escalável, abrangendo todas as implantações de IoT na cidade.

Exigiu-se uma demonstração de que a AIPD foi realizada de forma adequada. Também foi imposto um nível mínimo de transparência como a publicação de resultados e o envolvimento do usuário final na AIPD.

Uma AIPD poderia incluir um ou vários componentes de uma cidade inteligente, como um sistema de sensores, um banco de dados e um aplicativo que estavam ligados a um serviço de mobilidade urbana. Desse modo, a AIPD poderia avaliar múltiplas operações de tratamento de dados[448].

A última base do tripé do sistema de proteção de dados do *Synchronicity* é o *Privacy App*[449]. Pela dificuldade de obter o consentimento prévio e informado dos cidadãos para a coleta de seus dados pessoais, o processamento de dados pessoais em cidades inteligentes, geralmente, depende de outras bases legais.

No entanto, é necessário que o controlador de dados tome medidas eficazes para fornecer as informações sobre o tratamento de dados ao seu titular, de forma transparente e facilmente acessível. Ademais, é necessário que o controlador crie meios para o titular de dados exercer seus direitos.

Com efeito, o *Synchronicity* criou um aplicativo denominado *Privacy APP*, que ficou disponível gratuitamente para smartphones Android e iPhone em vários idiomas. O aplicativo

---

[447] ZIEGLER, Sébastien. **Internet of Things Security and Data Protection.** Springer. 2019 159 p.
[448] ZIEGLER, Sébastien. **Internet of Things Security and Data Protection.** Springer. 2019 161 p.
[449] PRIVACY APP. **Welcome to PrivacyApp!** Disponível em: https://www.privacyapp.info/

permitia que as cidades compartilhassem informações sobre a implantação de dispositivos em IoT nos espaços públicos.

O app fornecia um mapa que informava sobre cada dispositivo de IoT implantado na cidade, detalhando sobre a sua finalidade da coleta dos dados pessoais, o período de retenção daqueles dados e quem era o responsável pelo tratamento. O *Privacy APP* também fornecia aos titulares dos dados um meio de contato com o departamento responsável pelo tratamento de dados daquele dispositivo de IoT[450].

Por fim, o app permitia que os cidadãos identificassem aqueles dispositivos que não estavam catalogados no mapa do aplicativo. Assim, o cidadão tirava uma foto do dispositivo de IoT e marcava-o no mapa. Posteriormente, as informações adicionais sobre aquele dispositivo seriam complementadas pelo seu responsável.

Atualmente, a União Europeia está investindo no programa de investigação e inovação *Horizon Europe* para cidades inteligentes. A previsão de duração do programa é de até 2027 e tem como objetivo principal criar cidades inteligentes que não impactam na alteração climática.

3.5. *E-Learning Programme and Guide to Basic Anonymisation - Singapure*

Em Singapura, as operações que envolvem dados pessoais de indivíduos devem cumprir com o *Personal Data Protection Act*, de 2012 (PDPA). A principal autoridade sobre o assunto na cidade-estado é a *Personal Data Protection Commission* (PDPC).

Entre outras atribuições, a PDPC fiscaliza as operações que envolvem dados pessoais e promove as melhores práticas de proteção de dados pessoais. Ainda, o *Personal Data Protection Commission* representa o Governo de Singapura, inclusive a nível internacional, em questões relacionadas com dados pessoais[451].

O PDPC realiza atividades educativas e de divulgação gratuita para ajudar as organizações a compreender e aplicar a *Personal Data Protection Act*. Uma dessas atividades é o *E-Learning Programme*, que são formas de ensino sobre a PDPA por meio de ferramentas de aprendizagem interativas desenvolvidas pela própria PDPC[452].

A primeira ferramenta é o e-*Learning Programme on the PDPA* que oferece uma introdução geral da lei de proteção de dados pessoais de Singapura. A duração do curso é de,

---

[450]ZIEGLER, Sébastien. **Internet of Things Security and Data Protection.** Springer**.** 2019 165 p.
[451]PERSONAL DATA PROTECTION COMMISSION SINGAPORE – **Who we are.** Disponível em: https://www.pdpc.gov.sg/Who-We-Are/About-Us
[452]PERSONAL DATA PROTECTION COMMISSION SINGAPORE – **E-Learning Programme**. Disponível em: https://www.pdpc.gov.sg/Help-and-Resources/2018/01/E-Learning-Programme

aproximadamente, 60 minutos, e utiliza exemplos fictícios de empresas, produtos, logotipos, pessoas e eventos para mostrar como a PDPA é aplicada.

Outra ferramenta é O *DPO Challenge Game*, igualmente elaborada pela PDPC, que simula o papel do DPO em uma organização. A tarefa do jogador é realizar uma auditoria interna que garanta a prática de todas as medidas de precaução para a proteção de dados pessoais e a ciência de todos os funcionários da organização sobre as regras da PDPA. O jogo tem a duração de quarenta minutos.

O *Assessment Module* é uma ferramenta do PDPC de avaliação online com trinta questões que versam sobre o conhecimento da *Personal Data Protection Act.* A prova possui módulos exclusivos para as organizações que desejam aplicar e monitorar os resultados dos seus funcionários e para o DPO que deseja gerenciar a avaliação.

Outra iniciativa da *Personal Data Protection Commission* de Singapura foi o lançamento, em março de 2022, do *Guide to Basic Anonymisation,* um guia com orientações práticas, destinado às empresas, sobre a realização adequada de processos de anonimização dos dados pessoais. O guia ensina conceitos e técnicas básicas de anonimização de dados, além de oferecer um processo simples de anonimização para um conjunto de dados de organizações, dividido em cinco etapas[453].

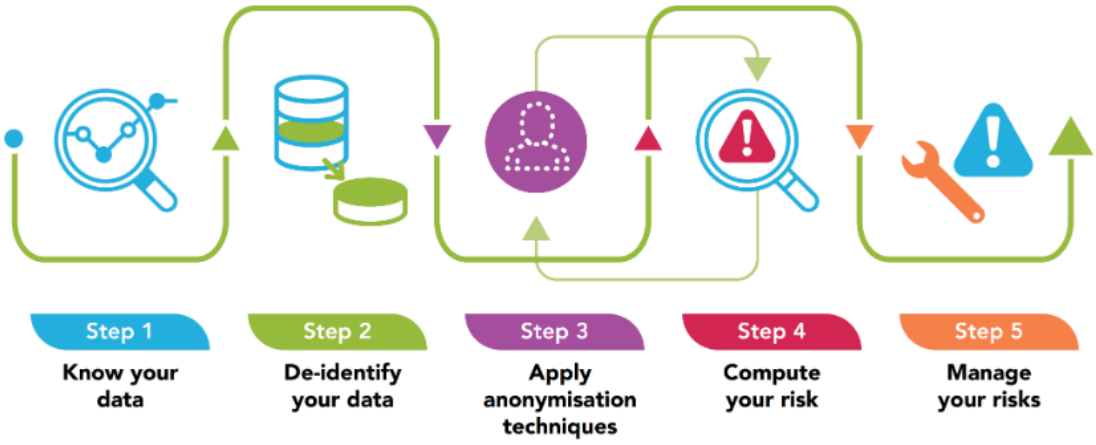

Figura 5: As cinco etapas do processo de anonimização dos dados do PDPC[454]

[453] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Basic Anonymization.** Disponível em: https://www.pdpc.gov.sg/Help-and-Resources/2018/01/Basic-Anonymisation

[454] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation.** Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 14 p.

Este processo de anonimização foi desenvolvido para cinco casos específicos, sendo dois deles para o compartilhamento interno de dados, um para dados desidentificados e o outro para dados anonimizados. Os demais casos são para o compartilhamento de dados externos, para dados sintéticos[455] e para retenção de dados por um longo período de tempo[456].

O *know your data* é o primeiro passo do processo de anonimização de dados da PDPC e consiste em classificar os atributos de dados pessoais, contidos no registro, entre os identificadores diretos e os identificadores indiretos. Nesta etapa, já ocorre a remoção dos atributos que não sejam necessários ao processo, em respeito à minimização dos dados[457].

A segunda etapa é a *de-identify your data* e se refere a remoção dos identificadores diretos como, nome e endereço de e-mail. Se houver a necessidade de utilizar identificadores diretos, o guia sugere a utilização de pseudônimo para cada um desses registros[458].

O *apply anonymisation techniques* é a etapa da qual as técnicas de anonimato são aplicadas aos identificadores indiretos. O objetivo é dificultar o processo de combinação dos dados registrados com outros conjuntos de informações adicionais que poderiam reidentificar os indivíduos titulares dos dados.

O guia da PDPC alerta que a aplicação das técnicas de anonimização modificará os valores dos dados, o que pode afetar a sua utilidade. A PDPC lista algumas técnicas de anonimização para cada um dos cinco casos estudados, mas não proíbe o uso de outras técnicas[459].

A quarta etapa é a *compute your risk* que é a medição do nível de risco de reidentificação de um conjunto de dados anonimizados. O nível de anonimização deve estar de acordo com o exigido no capítulo três do *PDPC's Advisory Guidelines on the Peronal Data Protection Act for Selected Topics*[460]

---

[455] São informações artificiais que podem ser usadas no lugar de dados reais. Geralmente, servem para treinar modelos de IA e testar softwares.

[456] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation**. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 15 - 17 p.

[457] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation**. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 18 - 19 p.

[458] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation** . Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 20 - 21 p.

[459] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation** . Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 22- 23 p.

[460] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **PDPC's Advisory Guidelines on the Peronal Data Protection Act for Selected Topics** Disponível em: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-selected-topics

Para o cálculo do risco de reidentificação, o PDPC sugere o uso da *k-anonymity,* uma metodologia usada para garantir que o limite de risco de reidentificação não seja ultrapassado. Esta metodologia pode não ser adequada para casos de uso complexos[461].

Por fim, a quinta etapa é o *manage your re-identification and disclousure risks* e determina a adoção de medidas adequadas para proteger os dados contra a reidentificação e divulgação. Os parâmetros utilizados no processo de anonimização devem ser documentados para futuras revisões e ajustes[462].

O *Personal Data Protecition Commission* também dispõe do *Data Anonymisation Tool,* ferramenta gratuita de anonimização de dados que ajuda as organizações a transformar os seus conjuntos de dados por meio de técnicas simples de anonimização. O arquivo da ferramenta também inclui um infográfico que orienta o uso do *Data Anonymisation Tool.* [463].

3.6. *Cybersecurity Certification e SME Cybersecurity – ENISA*

A União Europeia, através da *European Union Agency for Cybersecurity* (ENISA), está desenvolvendo um quadro de certificação de cibersegurança para produtos e serviços de TIC. A certificação de segurança formulada por uma agência pública visa trazer confiança ao mercado de produtos, serviços e processos de TIC da União Europeia e àqueles mercados estrangeiros que o adotarem.[464]

A segurança cibernética é um requisito primordial para o sucesso de uma cidade inteligente. Portanto, mesmo que a ENISA seja uma organização que não trata especificamente de *smart city,* ela tem um papel importante na sua implantação na União Europeia.

Essa certificação é um meio prático a ser adotado pela UE para auxiliar o fornecedor e o prestador de serviço de TIC a provar que estão em conformidade com a *Cybersecurity Act*. Também, ajudará a empresa de TIC a divulgar as medidas de segurança adotadas para o seu setor, desmonstrando que as soluções foram testadas, são resistentes a certos níveis de ataque e são tecnologias de proteção de última geração.

---

[461] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation** Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 49 p.

[462] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Bssic Anonymisation.** Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf 25 p.

[463] PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Basic Anonymisation Tool Now Available.** Disponível em: https://www.pdpc.gov.sg/News-and-Events/Announcements/2022/05/Data-Anonymisation-Tool-Now-Available

[464]EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Certification.** Disponível em: https://www.enisa.europa.eu/topics/certification

O certificado de cibersegurança em desenvolvimento pela ENISA terá o tempo de validade limitado e poderá ser prorrogado por meio de uma reavaliação. Os regimes de certificação de cibersegurança da UE vão criar o *Conformity Assessment Bodies*, mercado que irá fornecer serviços de certificação e ferramentas por toda a União Europeia[465].

O desenvolvimento de uma certificação a nível de UE também promove a harmonização do nível de segurança dos seus Estados-Membros, cujo o objetivo é capacitar o Mercado Único Digital da UE[466]. Para as empresas que possuem um certificado de cibersegurança, a ENISA fornecerá orientações para facilitar o processo de transição.

A estrutura de certificação de segurança cibernética desenvolvida pela ENISA, é baseada no *Cybersecurity Act*, e visa fornecer critérios de conformidade específicos, de acordo com o serviço ou produto de TIC. Desse modo, a certificação fornecerá um aviso aos usuários daquele produto ou serviço sobre o seu nível de conformidade de acordo com a lei.

O quadro de certificação de cibersegurança da UE estabelece o procedimento para a criação de sistemas de certificação e abrange produtos, serviços e processos de TIC. O quadro terá três níveis de garantia de segurança, sendo eles baixo, médio e grande, com base no nível de risco da utilização do produto ou serviço[467].

Atualmente, a ENISA está desenvolvendo três regimes de certificado de cibersegurança, sendo eles: o *European Cybersecurity Certification Scheme on Commom Criteria* (EUCC) voltado para produtos de TIC, como produtos e componentes de *hardware* e *software*; o *European Certification Scheme for Cloud Services* (EUCS), destinado a produtos e serviços baeados em *cloud* e; o *European Certification Scheme for* 5G (EU5G) para as redes 5G[468].

Insta destacar que há uma discussão acerca da criação de um processo de certificação direcionado para o mercado de empresas de TIC que desenvolvem produtos e serviços baseados em intelgiencia artificial.

---

[465] EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Learn more about UE Cybersecurity Certification.** Disponível em: https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq

[466] EUROPEAN UNION AGENCY FOR CYBERSECURITY. **UE Cybersecurity Certification.** Disponível em: https://certification.enisa.europa.eu/

[467] EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Cybersecurity Certification Framework. The goal of Cybersecurity Certification Framework.** Disponível em https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework

[468] EUROPEAN UNION AGENCY FOR CYBERSECURITY. **UE Cybersecurity Certification.** Disponível em: https://certification.enisa.europa.eu/

Outra iniciativa da ENISA é o programa *SME Cybersecurity* para empresas de pequeno e médio porte. Este mercado representa mais da metade do PIB europeu e emprega mais de 100 milhões de pessoas[469].

Durante a pandemia COVID 19, muitas empresas de menor tamanho foram obrigadas a usarem serviços de tecnologia para continuar operando. Alguns deles são serviços em *cloud,* compra e venda pela internet e realocação de funcionários para o trabalho remoto.

Por conta da necessidade atual desse mercado, a ENISA realizou uma pesquisa para investigar quais eram os incidentes cibernéticos mais comuns contra as empresas de pequeno e médio porte. Por meio de entrevistas com os empreendedores, a ENISA constatou que os crimes mais comuns eram os ataques de *rasomware,* o roubo de computadores portáteis, ataques de *fishing* e fraude.

Ainda, 90% dos entrevistados afirmaram que as questões de cibersegurança implantadas após a ocorrência dos delitos tiveram graves impactos negativos nos seus negócios. O baixo orçamento de segurança, a falta de competências cibernéticas e o aumento dos ataques cibernéticos afetaram a competitividade das empresas de médio e pequeno porte.

Por conta desse cenário, a ENISA criou uma série de orientações para ajudar essas empresas a enfrentar a mudança digital, acelerada pela pandemia COVID-19, e um guia, contendo doze passos para melhorar a segurança cibernética da empresa[470]. Também foi criado o *Ad-Hoc Working Group on Enterprise Security* para orientar os Estados-Membros a adotarem medidas de proteção para as empresas de pequeno e médio porte como política de cibersegurança, capacitação, sensibilização e gestão de riscos[471].

---

[469] EUROPEAN UNION AGENCY FOR CYBERSECURITY. **SME Cybersecurity** Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

[470]EUROPEAN UNION AGENCY FOR CYBERSECURITY. **SecureSME**. Disponível em: https://www.enisa.europa.eu/securesme#/

[471]EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Ad-Hoc Working Group on Enterprise Security.** Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity/ad-hoc-working-group-enterprise-security

CONCLUSÃO

Em resposta à pergunta principal desse estudo, a primeira peculiaridade encontrada da proteção de dados pessoais em cidade inteligente é a ausência de normas específicas sobre o tema no Brasil. Mesmo com a eventual aprovação do projeto de lei de nº 976/21 (PNCI), não há perspectiva sobre o surgimento de regra específica de proteção de dados pessoais para o ambiente tecnológico urbano, haja vista a omissão declaradamente expressa do legislador do projeto neste sentido.

Isto acarreta um desafio de adequação do sistema de proteção de dados pessoais brasileiro, especialmente da LGPD. A ANPD e a comunidade jurídica terão um papel fundamental, tanto na garantia dos direitos e liberdades civis na cidade inteligente como na promoção da inovação tecnológica urbana.

A segunda peculiaridade identificada é os diferentes entendimentos de cada país sobre a proteção de dados pessoais e a privacidade. Ademais, a implantação tecnológica nas cidades está ocorrendo de forma global, com a ajuda de empresas estrangeiras que possuem culturas de proteção de dados distintas do local de implantação da tecnologia.

Em alguns casos, as empresas estrangeiras armazenam os dados pessoais em localidade diversa do país originário daquelas informações, o que dificulta a fiscalização das operações de tratamento, além de trazer um risco à soberania do país de origem. A empresa estrangeira pode ser demandada pelo seu governo a fornecer os seus dados pessoais.

O Direito internacional vem promovendo medidas para mitigar estes problemas, a exemplo do acordo de transferência de dados pessoais entre Europa e Estados Unidos, citado neste estudo, e da reforma legislativa australiana para o fortalecimento das regras de proteção de dados pessoais e de privacidade[472]. Ainda, destacam-se as *Standard Contractual Clauses,* também aqui estudadas, como uma medida protetiva dos dados pessoais e da privacidade em caso de operações de empresa estrangeira ordenada por um sistema legislativo de nível de proteção inferior.

Outra peculiaridade encontrada foi a identificação de limitações técnicas para oferecer mecanismos que respeitem as imposições do sistema de proteção de dados pessoais em *smart city,* especialmente as tecnologias de *big data* e IoT. Um exemplo de limitação do *big data* é a

[472]AUSTRALIAN GOVERNMENT. Attorney-General's Department. **Government response to the Privacy Act Review Report.** Disponível em: https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

dificuldade de identificar as informações consistentes e as utilizar conforme a necessidade de cada setor público.

Todavia, a limitação técnica mais preocupante do *big data* é a dificuldade de conciliar o seu volume, cada vez maior de dados, com os princípios da LGPD, especialmente com a minimização, a finalidade, a transparência e a qualidade dos dados. Conforme estudado, é da natureza do *big data* coletar o maior número de dados possíveis, o que pode comprometer a observância do sistema de proteção de dados pessoais.

Algumas medidas encontradas para mitigar a incompatibilidade do *big data* com a LGPD são: o desenvolvimento de tecnologia de armazenamento local de dados; o incentivo às espécies legais de uso secundário dos dados pessoais, como o compartilhamento de dados; a utilização de técnicas de anonimização dos dados pessoais e; o treinamento de pessoal que alimenta o banco de dados em situações como a I~HD.

Outro exemplo técnico diagnosticado é o risco à privacidade em sistemas de *smart city* para cidades, especialmente aqueles baseados em IoT, por falta de transparência do tratamento de dados pessoais, assimetria de informação e ausência de um nível aceitável de segurança para os dados pessoais. Ainda, cita a limitação tecnológica em garantir o direito à portabilidade dos dados pessoais do cidadão nas tecnologias *cloud* e *big data*.

Conforme estudado, a imposição do *Privacy By Design* aos desenvolvedores de tecnologia tem sido adotada nos principais sistemas de proteção de dados estrangeiros como um dos meios para promover a inovação responsável. Também, a confecção de regulamentos específicos, como o *Children's Code*, é um caminho para aprimorar o nível de segurança de dados pessoais sensíveis.

Além disso, destaca programas de conscientização que abordam, entre outros assuntos, as legislações de proteção de dados pessoais, a sua importância para o indivíduo e para o coletivo, a sua aplicação prática e as técnicas de anonimização de dados pessoais. Um exemplo disso é o *E-Learning Programme* de Singapura e suas ferramentas criativas, simples de manusear e acessíveis a todos.

Também, constatou-se a importância da participação popular nos projetos de implantação da tecnologia no ambiente urbano através de audiências públicas. É primordial haver debates entre os componentes sociais e os desenvolvedores de tecnologia sobre, especialmente, os benefícios da implantação tecnológica no ambiente urbano, os riscos, trazidos pela tecnologia, aos direitos e às liberdades civis, as medidas de prevenção e de inclusão de grupos menos favorecidos no ambiente tecnológico.

No âmbito organizacional, é fundamental a construção de uma ética empresarial, que se preocupa não apenas com os elementos ligados diretamente à empresa, mas com todos aqueles que com ela se relaciona, seja de forma econômica ou não (os *stakeholders* em geral)[473]. A empresa de TIC que criar produto ou prestar serviço para uma cidade, observando valores, como, o bem-estar do cidadão e a preservação do meio ambiente, terá maior chance de sobreviver ao mercado, cada vez mais exigente e monitorado por todos os componentes sociais.

Por fim, destaca o projeto da ENISA sobre a certificação para o setor de cibersegurança, buscando unificar as medidas protetivas adotadas pelas empresas da União Europeia. Esta ação confere segurança jurídica às empresas e confiabilidade do mercado.

Outra peculiaridade identificada foi o risco de monitoramento excessivo sobre a vida dos cidadãos, que pode ser protagonizado tanto pelas empresas privadas como pelos governos. Com a inserção massiva da tecnologia no cotidiano do ser humano, as formas de monitoramento foram potencializadas.

Esta peculiaridade proporciona desafios de fiscalização sobre os responsáveis pela coleta e pelo uso dos dados pessoais nas cidades inteligentes. Como constatado neste estudo, o volume crescente de serviços e produtos de TIC pode causar uma sobrecarga nos órgãos de fiscalização.

Ademais, deve-se encontrar o grau correto da medida punitiva contra o tratamento de dados pessoais ilegal, devendo ser observados os direitos do cidadão e a promoção da inovação tecnológica. As autoridades devem aplicar uma sanção eficaz, de forma a desestimular a conduta ilegal, mas, ao mesmo tempo, não excessiva, que não prejudique a inovação tecnológica.

Um caminho para a estruturação das operações com dados pessoais no ambiente público é a formação de um organograma semelhante ao Duplo DPO, já abordado no texto. Cada cidade teria um Coordenador público de DPO's, responsável pela gestão dos DPO's das entidades públicas.

Diante da recente implantação de tecnologias de *smart city* no Brasil e como forma de contribuir com a realização de outras pesquisas jurídicas nesta área, sugere-se que os próximos estudos jurídicos tenham por objeto os seguintes temas: 1) a privacidade na implantação de tecnologia *smart city* em cidades inteligentes; 2) o tratamento de dados pessoais sensíveis em tecnologia de *smart city*, notadamente para o setor público de saúde; 3) a cibersegurança para a implantação da tecnologia *smart city* em espaços públicos; 4) a estrutura pública municipal

[473] DE LUCCA, Newton. **Da Ética Geral à Ética Empresarial**. Editora Quartier Latin. 2009. 338-339 p.

brasileira de proteção de dados pessoais (já que notoriamente a estrutura fática, orçamentária e de pessoal em inúmeros municípios brasileiros é assaz diversa daquela existente no âmbito federal) e; 5) o modelo contratual brasileiro sobre regras de proteção de dados pessoais para empresas estrangeiras de tecnologia *smart city* para cidades.

REFERÊNCIAS

ABRUSIO, Juliana; MARANHÃO, Juliano; CAMPOS, Ricardo; LÓPEZ, Nuria**. Dados de Geolocalização e a investigação de Marielle Franco.** 07/07/2020. Disponível em: https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle/

AMNESTY INTERNATIONAL **Big Brother Watch and others vs the United Kingdom** (Applications N. 58170/13, 62322/14 and 24960/15). 2018. Disponível em: https://policehumanrightsresources.org/big-brother-watch-and-others-vs-the-united-kingdom

ARRAY OF THINGS. **Array of Things Governance & Privacy Policies**. Disponível em: https://arrayofthings.github.io/privacypolicy.html

ARRAY OF THINGS. **Sage.** Disponível em*:* https://arrayofthings.github.io/

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Disponível em https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos

AUSTRALIAN GOVERNMENT. Attorney-General's Department. **Government response to the Privacy Act Review Report.** Disponível em: https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

AUSTRALIAN GOVERNMENT. **Office of the Australian Information Commissioner. Privacy By Design** Disponível em: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/privacy-by-design

AUTONOMOUS READY. **El caso Barcelona.** Disponível em: https://autonomousready.org/caso-barcelona/

BARCELONA. **Agreement to drive the Mobility of the future**. 27.06.2022. Info Barcelona. Disponível em: https://www.barcelona.cat/infobarcelona/en/tema/smart-city/agreement-to-drive-the-mobility-of-the-future_1190154.html

BANCO CENTRAL DO BRASIL. **BC aprimora mecanismos de segurança do PIX**. Banco Central do Brasil 29/09/2021. Disponível em: https://www.bcb.gov.br/detalhenoticia/581/noticia

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 85 de 08/04/2021**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85

BAMBROUGH, Billy. **Apple Card é acusado de discriminação contra mulheres.** Forbes. 11/11/2019 Disponível em: https://forbes.com.br/forbes-mulher/2019/11/apple-card-e-acusado-de-discriminacao-contra-mulheres/

BASÍLIO, Patrícia. **BC confirma vazamento de 395 mil chaves PIX sob responsabilidade da BANESE**. G1 Portal de notícias da Globo. 30/09/2021. Disponível em:. https://g1.globo.com/economia/noticia/2021/09/30/bc-confirma-vazamento-de-395-mil-chaves-pix-de-clientes-do-banese.ghtml

BIASI, Danielle Portugal de. **Propriedade: reconstruções na era do acesso e compartilhamento.** 6ª edição. Indaiatuba, SP. Editora Foco 2022

BIONI, Bruno Ricardo. **Proteção de Dados- Contexto, narrativas e elementos fundantes** BIONI Data Privacy Specialist.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais. A função e os limites do consentimento.** 2019. Editora Forense LTDA.

BLACKWELL, Theo; THOMSON, Julia. **Smart London Together Roadmap 2018-21.Report back to Mayor of London** . October 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.london.gov.uk/sites/default/files/slt_roadmap_summary_paper_for_2021.pdf

BLUME, Peter. **The Data Subject**. 2015

BRASIL. Autoridade Nacional de Proteção de Dados. **Estudo preliminar. Hipóteses legais de tratamento de dados pessoais: Legítimo interesse**. Setembro/2022. Versão 1.0. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/aberta-tomada-de-subsidios-sobre-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/2022.09.06_EstudoTcnicoCrianaseAdolescentes.pdf

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais**. Brasília: maio/2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf>.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo. Tratamento de dados pessoais pelo Poder Público.** Versão 2.0. junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais **Incidentes de segurança com dados pessoais.** Ministério da Justiça e Segurança Pública. 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais#:~:text=Um%20incidente%20de%20seguran%C3%A7a%20com,dados%20inadequada%20ou%20il%C3%ADcita%2C%20os

BRASIL. Autoridade Nacional de Proteção de Dados. **Publicado relatório do ciclo de Monitoramento da ANPD.** 18/08/2023. Disponível em*:* https://www.gov.br/anpd/pt-br/assuntos/noticias/publicado-relatorio-do-ciclo-de-monitoramento-da-anpd

BRASIL. Autoridade Nacional de Proteção de Dados. **RADAR TECNOLÓGICO. ANPD lança nova série de publicações técnicas.** 29/01/2024. Disponível em**:** https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-serie-de-publicacoes-tecnicas-com-o-tema-cidades-inteligentes

BRASIL. Câmara dos Deputados. Projeto de lei 976.2021. **Política Nacional de Cidades Inteligentes (PNCI).** Disponível em: https://www.camara.leg.br/propostas-legislativas/2274449

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL Presidência da República. Decreto nº 9.637, de 26 de dezembro de 2018**. Plano Nacional de Segurança da Informação.** Diário Oficial da União 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm

BRASIL Presidência da República. Decreto nº 9.854, de 25 de junho de 2019. **Plano Nacional de Internet das Coisas.** Diário Oficial da União 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm

BRASI. Presidência da República. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Diário Oficial da União. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

BRASI. Presidência da República. Lei nº 10.257, de 10 de julho de 2001**. Estatuto da cidade**. Diário Oficial da União. 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm

BRASIL. Presidência da República. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Diário Oficial da União. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Presidência da República. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação**. Diário Oficial da União. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

BRASIL, Presidência da República Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. 15/08/2018. Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 64.941-RJ** (2022/0284473-3). Agravante: G.B.I. L. e outros. Agravado: Ministério Público do Estado do Rio de Janeiro. Relator: Ministro Rogério Schietti Cruz. Brasília, 18 de abril de 2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1262917027/inteiro-teor-1262917112

BRASIL. Superior Tribunal Federal. **Entenda a condenação dos réus pelos atos antidemocráticos de 8 de janeiro.** 25/10/2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=518984&ori=1

BRASIL Supremo Tribunal Federal. **Partidos questionam norma que condiciona fornecimento de dados à Abin a ato presidencial.** Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449429&ori=1

BRASIL. Superior Tribunal Federal. **Relator divulga balanço dos processos relacionados aos atos antidemocráticos de 8/1.** 13/09/2023 Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=513973&ori=1

BRASIL. Supremo Tribunal Federal. **STF suspende compartilhamento de dados de usuários de telefonias com IBGE.** 07/05/2020. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1

BRASIL. Supremo Tribunal Federal. **STF valida compartilhamento de dados mediante requisitos. O Plenário também fixou restrições à atuação do Comitê Central de Governança de Dados.** 20/10/2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Banco de Dados e Cadastros dos Consumidores.** Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/bancos-de-dados-e-cadastros-de-consumidores

BRAUNEIS, Robert; GOODMAN, Ellen P. **Algorithmic Transparency for the Smart City. Yale Journal of Law & Technology.** Vol. 20. 2018. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://yjolt.org/sites/default/files/20_yale_j._l._tech._103.pdf.

CAPITAL ONE. **Information on the Capital One cyber incident.** Disponível em: https://www.capitalone.com/digital/facts2019/

CASTELLS, Manuel. **A era da informação: Economia, sociedade e cultura. A sociedade em rede.** Vol., 1. Ed. Paz e Terra LTDA, São Paulo. 1999

CATE, Fred H. DEMPSEY, James X. ***Bulk Collection: Systematic Government Access to Private- Sector Data.*** OXFORD. 2017.

CCDCOE. **EU Data Retention Directive Union**. Disponível em: https://ccdcoe.org/incyder-articles/eu-data-retention-directive-invalid/#footnote_1_2661

CERULLO, Megan. **How companies get inside gig workers' heads with "algorithmic wage discrimination".** CBS NEWS. 18/04/2023. Disponível em https://www.cbsnews.com/news/algorithmic-wage-discrimination-artificial-intelligence/

CHERTOV, Oleg. MYLOVANOV Tymofiy; KONDRATENKO, Yuriy e outros. **Recent Developments in Data Science and Intelligent Analysis of Information.** Editora Springer. June 4-7,2018

CHRISTENSEN, Clayton M.; RAYNOR, Michael E.; MCDONALD, Rory. **What is disruptive innovation?** Harvard Business Review. 2015

CITY OF ADELAIDE. **Smart Bins to Keep Adelaide's Streets Cleaner**. Disponível em*:* https://www.cityofadelaide.com.au/media-centre/smart-bins-to-keep-adelaides-streets-cleaner/

CITY OF ADELAIDE. **Smart city Adelaide.** Disponível em*:* https://www.cityofadelaide.com.au/about-adelaide/smart-city-adelaide/

CITY OF DARWIN. **Switching on Darwin.** Disponível em: https://www.darwin.nt.gov.au/transforming-darwin/innovation/switching-on-darwin

CNBC. **Europe and the U.S.finally agree a landmark data-sharing pact - -and it's already under threat.** 12/07/2023. Disponível em: https://www.cnbc.com/2023/07/12/eu-and-us-agree-new-data-sharing-deal-what-is-it-and-why-it-matters.html

COELHO, Henrique; NASCIMENTO, Rafael; ALVES, Raoni. **Mulher presa após reconhecimento facial é solta**. **Mandado de prisão já tinha sido cumprido**. G1 Portal de notícias da Globo. 04/01/2024 Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/01/04/mulher-presa-apos-reconhecimento-facial-e-solta-mandado-de-prisao-ja-tinha-sido-cumprido.ghtml

COHEN, Boyd. **The 3 Generations of Smart Cities. Fast Company.** 08/10/2015. Disponível em: https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities Acesso em 10/01/2023

COMITÊ DE GOVERNANÇA DIGITAL. **Programa de Governança em Privacidade**. Escola Nacional de Administração Pública. Versão 1.0. julho/2021. Brasília-DF. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.enap.gov.br/bitstream/1/6480/1/Programa%20de%20Governan%C3%A7a%20em%20Privacidade%20da%20Enap_PGP-Enap.pdf

CONGRESS.GOV. H.R.3386 - **Smart Cities and Communities Act of 2021.** 117th Congress (2021-2021) disponível em: https://www.congress.gov/bill/117th-congress/house-bill/3386?s=1&r=11

CONGRESS.GOV. **S.686 - Restrict Act.** 2023. Disponível em: https://www.congress.gov/bill/118th-congress/senate-bill/686?s=1&r=15

COURT OF JUSTICE OF THE EUROPEAN UNION**. The Court of Justice declares the Data Retention Directive to be invalid.** Luxembourg, 8/04/2014. Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

CRAVO, Daniela Copetti. **Direito à Portabilidade de Dados: Necessidade de Regulação EX ante e EX post.** Tese de Doutorado. Universidade Federal do Rio Grande do Sul. 2018. Porto Alegre. Disponível em: https://lume.ufrgs.br/handle/10183/180184

CRÓ, Isabel, ROEGIERS, Tristan Castro. **Data Protection in the Smart City Of Lisbon**. Flanders, Investiment & Trade – Lisbon. 2021 Disponível em: https://www.flandersinvestmentandtrade.com/export/sites/trade/files/market_studies/2021-Portugal-Data%20protection%20in%20the%20smart%20city%20of%20Lisbon-Website_2.pdf

CUNHA, Maria Alessandra, PRZEYBILOVICZ, Erico, MACAYA, Javiera Fernanda Medina, BURGOS, Fernando. **SMART CITIES: Transformação digital nas cidades**. FGV. 1ª edição. São Paulo. Programa Gestão Pública e Cidadania. 2016

D AMICO, Gaspare; L ABBATE, Pasqua; LIAO, Wenjie; **Understading Sensor Cities: Insights From Technology Giant Company Driven Smart Urbanism Practices**. MDPI. Disponível em: https://www.mdpi.com/1424-8220/20/16/4391

DATAREPORTAL. **TikTok users, stats, data & trends.** 11/05/2023 Disponível em: https://datareportal.com/essential-tiktok-stats

DAVIS, Jessica. **Phishing attack on Torrance Memorial puts patient records at risk.** Healthcare IT News. 20/60/2017. Disponível em: https://www.healthcareitnews.com/news/phishing-attack-torrance-memorial-puts-patient-records-risk.

DE LUCCA, Newton. **Da Ética Geral à Ética Empresarial**. Editora Quartier Latin. 2009.

DIÁRIO DA REPÚBLICA. **Princípio da minimização (tratamento de dados pessoais)** disponível em: https://diariodarepublica.pt/dr/lexionario/termo/principio-minimizacao-tratamento-dados-pessoais

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais. Fundamentos da Lei Geral de Proteção de Dados.** Revista dos Tribunais. 2ª edição. 2020.

DTG. **Qué es DTG 3.0**. Disponível em: https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/dgt-3.0/

ECONOMIST IMPACAT. **digital cities index.** 2022. Disponível em: https://impact.economist.com/projects/digital-cities/2022-executive-summary/?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=19495686130&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=CjwKCAiAwomeBhBWEiwAM43YIF84K7JDoD_XaHdKyRl91Mk2VXqHTrDaLX_7yLtARAJ77npYvMjMARoCGaAQAvD_BwE&gclsrc=aw.ds

ECO RENEWABLE ENERGY. **Transforming Cities, Empowering Communities: 7 Smart Cities Australia Projects.** Disponível em: https://www.ecorenewableenergy.com.au/articles/building-smart-cities-australia-6-notable-projects/

EDWARDS, Lilian. **Privacy, security and data protection in smart cities: a critical EU law perspective.** 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711290

EKATHIMERINI. **Mobile phone operator slapped with fine over data breach.** Disponível em: https://www.ekathimerini.com/economy/1176648/mobile-phone-operator-slapped-with-fine-over-data-breach/

ENISA. **European Electronic Communications Code** Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-policy/european-electronic-communications-code

ENISA. **Telecom Security Incidents 2021.** 27/07/2022. Disponível em: https://www.enisa.europa.eu/publications/telecom-security-incidents-2021

EURONEWS. **Quais países que proibiram o TikTok e porquê?** 27/03/2023 Disponível em: https://pt.euronews.com/next/2023/03/27/quais-os-paises-que-proibiram-o-tiktok-e-porque

EURONEWS. **UE dá luz verde para partilha de dados pessoais com os EUA**. 10/07/2023. Disponível em: https://pt.euronews.com/my-europe/2023/07/10/ue-da-luz-verde-para-partilha-de-dados-pessoais-com-os-eua.

EUROPA PARLIAMENT. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf

EUROPEAN COMMISSION. **Communication from the commission to the European Parliament, the council, the European economic and social committee and the committee of the regions**. Brussels, 19.02.2020 Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

EUROPEAN COMISSION: **Horizon 2020. Details of the UE funding programme which ended in 2020 and links to further information** Disponível em: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en

EUROPEAN COMMISSION. **Standard Contractual Clauses (SCC)** 04/06/2021. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

EUROPEAN COMMISSION. **SynchroniCity. Delivering an IoT enabled Digital Single Market for Europe and Beyond.** Disponível em: https://cordis.europa.eu/project/id/732240

EUROPEAN COURT OF HUMAN RIGHTS. **Big Brother Watch and others v the United Kingdom.** Disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13278%22]}

EUROPEAN COURT OF HUMAN RIGHTS. **Convenção Europeia dos Direitos do Homem**. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por

EUROPEAN DATA PROTECTION SUPERVISOR. **Data minimization.** Disponível em https://edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=Data%20minimization,necessary%20to%20fulfil%20that%20purpose.

EUROPEAN DATA PROTECTION BOARDING. **Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation.** Disponível em: https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en

EUROPEAN UNION. **European Parliament. Regulation nº 2016/679/CE**. Brussels. 27/04/2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

EUROPEAN UNION AGENCY FOR CIBERSECURITY. Disponível em: https://www.enisa.europa.eu/

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Ad-Hoc Working Group on Enterprise Security.** Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity/ad-hoc-working-group-enterprise-security

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Certification.** Disponível em: https://www.enisa.europa.eu/topics/certification

EUROPEAN UNION AGENCY FOR CIBERSECURITY. *Cloud Security for Healthcare Services.* 18/01/2021. Disponível em: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Cybersecurity Certification.** Disponível em: https://certification.enisa.europa.eu/

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Cybersecurity Certification Framework. The goal of Cybersecurity Certification Framework.** Disponível em https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Learn more about UE Cybersecurity Certification.** Disponível em: https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **SecureSME.** Disponível em: https://www.enisa.europa.eu/securesme#/

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **SME Cybersecurity** Disponível em: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

EUROPEAN UNION LAW. **Directiva (UE) 2018/1972 Do Parlamento Europeu e Conselho de 11 de dezembro de 2018.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32018L1972

EUROPEAN UNION LAW. **Directive 2006/24/EC**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1405060274756&uri=CELEX:32006L0024

FILAY, Steven. **Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods.** *2014*

FORBES. **What Smart Cities are Learning from Smart Farms**. 27/11/2019. Disponível em: https://www.forbes.com/sites/bayer/2019/11/27/what-smart-cities-are-learning-from-smart-farms/?sh=7d71342fac64

FRAGOSO, Roberto. **Comissão de juristas debate discriminação tecnológica por inteligência artificial**. Senado Federal 12/05/2022 disponível em: https://www12.senado.leg.br/radio/1/noticia/2022/05/12/comissao-de-juristas-da-inteligencia-artificial-debate-discriminacao-tecnologica

FRASÃO, Ana, **Discriminação algorítmica. Compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade - parte 1.** 16/06/2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://professoraanafrazao.com.br/files/publicacoes/2021-06-16-Discriminacao_algoritmica_Compreendendo_o_que_sao_os_julgamentos_algoritmicos_e_o_seu_alcancena_atualidade_Parte_I.pdf Acesso em: 10/05/2023

FUTUREBUILT. **What is FutureBuilt**. Disponível em: https://www.futurebuilt.no/English.

FUTUREBUILT. **Landbrukskvartalet, Oslo.** Disponível em: https://www.futurebuilt.no/English/Pilot-projects?municipal%5B%5D=oslo&function%5B%5D=infrastructure&function%5B%5D=neighbourhoods#!/English/Pilot-projects/Landbrukskvartalet-Oslo

GLOBAL FREEDOM OF EXPRESSION. **Big Brother Watch v. United Kingdom**. Columbia University. Disponível em: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/

GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e Outros. **Guidelines for SynchroniCity architecture**. disponível em: https://cordis.europa.eu/project/id/732240/results

GORIN, Eisner. **The third-party doctrine and the fourth amendment**. 08/12/2023. Disponível em https://www.thefederalcriminalattorneys.com/third-party-doctrine

GRÖNLUND, Åke. **Electronic government: design, applications & management**. Hershey: Idea Group Publishing, 2002,

HALPIN, Padraic. **Meta hit with record $1.3 bin fine over data transfers.** REUTERS. 22/05/2023. Disponível em: https://www.reuters.com/technology/facebook-given-record-13-bln-fine-given-5-months-stop-eu-us-data-flows-2023-05-22/

HAVARD LAW REVIEW. **State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessment in Sentences.** 2016. Disponível em: https://harvardlawreview.org/print/vol-130/state-v-loomis/

HEALTHMANEGEMENT. **The Reuse of Health Data: Governance and Trust As Catalysers for quality**. Disponível em https://healthmanagement.org/c/healthmanagement/issuearticle/the-reuse-of-health-data-governance-and-trust-as-catalysers-for-quality

HOEREN, Thomas, RAISER-KOLANY, Barbara. **Big Data in Context Legal, Social and Technological Insights.** Springer Open. 2018.

HON, W. Kuan; MILLARD, Christopher; WALDEN, Ian, **The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated*?*** The Cloud of Unknowing, Part 1 (March 10, 2011). International Data Privacy Law (2011) 1 (4): 211-228, Queen Mary School of Law Legal Studies Research Paper No. 75/2011, Available at SSRN: https://ssrn.com/abstract=1783577 or http://dx.doi.org/10.2139/ssrn.1783577

INFORMATION COMISSIONER'S OFICE. **Public London Charter**. disponível em https://www.london.gov.uk/publications/public-london-charter

INFORMATION COMMISSIONER'S OFFICE. **Best interests of the child self- assessment.** Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/

INFORMATION COMISSIONER S OFFICE. **Big data, Artificial Intelligence, Machine Learning and Data Protection**. Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

INFORMATION COMMISSIONER'S OFFICE. **Code standards.** Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/

NFORMATION COMMISSIONER'S OFFICE. **Find the right resource**. Disponível em: https://ico.org.uk/for-organisations/advice-for-small-organisations/find-the-right-resource/

IINFORMATION COMISSIONER'S OFFICE. **Fines TikTok £12.7 million for misusing children's data.** 04/04/2023. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/

INFORMATION COMMISSIONER'S OFFICE **How to write a privacy notice and what goes in it.** Disponível em: https://ico.org.uk/for-organisations/advice-for-small-organisations/how-to-write-a-privacy-notice-and-what-goes-in-it/

INFORMATION COMMISSIONER'S OFFICE. **Introduction to the Childre's code**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/

INFORMATION COMMISSIONER'S OFFICE. **The Children's code and education Technologies (edtech).** Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/

INFORMATION COMMISSIONER'S OFFICE. **Instaling CCTV? Things you need to do first.** Disponível em*:* https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/installing-cctv-things-you-need-to-do-first/

INFORMATION COMMISSIONER'S OFFICE. **Your beginner's guide to data protection.** Disponível em: https://ico.org.uk/for-organisations/advice-for-small-organisations/your-beginner-s-guide-to-data-protection/

INFORMATION TECHNOLOGY GARTNER GLOSSARY. **Big Data.** Disponível em https://www.gartner.com/en/information-technology/glossary/big-data

INTERNATIONAL COMMISSIONER'S OFFICE. **Big Data and Data Protection.** Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220 Acesso em 29/04/2023

INTERNATIONAL TELECOMMUNICATION UNION. **Smart sustainable cites: Na analysis of definitions.** Focus Group Technical Report. 2014.

INTERSOFT CONSULTING. **GDPR. Privacy By Design.**Disponível em: https://gdpr-info.eu/issues/privacy-by-design/#:~:text=GDPR%20Privacy%20by%20Design&text=The%20term%20%E2%80%9CPrivacy%20by%20Design,in%20the%20technology%20when%20created.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Comitê de estatísticas sociais.** 2023. Disponível em: https://ces.ibge.gov.br/apresentacao/portarias/200-comite-de-estatisticas-sociais/base-de-dados/1146-censo-demografico.html#:~:text=O%20Censo%20Demogr%C3%A1fico%20tem%20por,ou%20de%20qualquer%20n%C3%ADvel%20de

IRWIN, Lucas. **Chatt app Knuddles fined £20.000 for GDPR breach.** IT Governance. 29/11/2018. Disponível em: https://www.itgovernance.eu/blog/en/chat-app-knuddels-fined-e20000-for-gdpr-breach

JOELSONS, Marcela. **Lei Geral de Proteção de Dados. Fronteiras do Legítimo Interesse**. Indaiatuba, SP. Editora Foco. 2022. Edição do Kindle.

JONNAVITHULA, Ani; SAYED, Pantho. **The TikTok Bill Isn't Only About TikTok.** Jolt Digest. 26/04/2023. Disponível em: https://jolt.law.harvard.edu/digest/the-tiktok-bill-isnt-only-about-tiktok

JUSTIA US LAW. **CLU v. Clapper.** No. 14-42 (2d Cir. 2015) Disponível em: https://law.justia.com/cases/federal/appellate-courts/ca2/14-42/14-42-2015-10-29.html

KASPERSKY. **Incident response analyst report.** 2021. Disponível em: https://securelist.com/the-nature-of-cyber-incidents/107119/

KASPERSKY. **Ransomware: definição, prevenção e remoção**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware

KITCHIN, Rob. **Data Driven, networked urbanism.** The Programmable City WP 14. Agosto de 2015. Disponível em: http://www.spatialcomplexity.info/files/2015/08/SSRN-id2641802.pdf Acesso em 10/05/2023.

KITCHIN, Rob. **The Real-Time City? Big Data and Smart Urbanism** (July 3, 2013). GeoJournal 79(1):1-14, 2014, Available at SSRN: https://ssrn.com/abstract=2289141 or http://dx.doi.org/10.2139/ssrn.2289141

LENCIONI, Sandra. **Observações sobre o conceito de Cidade e Urbano.** GEOUSP – Espaço e Tempo. São Paulo, n º 24, 2008

LEONARDI, Marcel. **Principais bases legais para o tratamento de dados pessoais no setor privado**. Caderno especial LGPD. 2019. Editora RT. São Paulo

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. De acordo com a lei geral de proteção de dados (lei N 13.709/2018 e as alterações da lei n.13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alterações do CDC (PL.3514/2015).** Editora Almedina. São Paulo. 2020

LIMA, Gabriel Ribeiro de. **Proteção de Dados em Cidade inteligente: o caso Sidewalk Labs (Google) em Toronto.** Editora Dialética LTDA. 2023

LIRA, Ricardo Pereira. **Direito Urbanístico, Estatuto da Cidade e regularização fundiária**. Revista de Direito da Cidade. Vol. 1. Disponível em: < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.e-publicacoes.uerj.br/index.php/rdc/article/viewFile/10493/8265>

MACIEL, Rafael Fernandes. **Manual prático da LGPD (lei nº 13.709/18).** Digital education. 1º edição. 2019.

MADHANI, Aamer. **Chicago begins Building "fitness tracker" to check its vitals.** 29/08/2016. USA Today. Disponível em: https://eu.usatoday.com/story/news/2016/08/29/chicago-begins-building-fitness-tracker-check-its-vitals/89434620/

MADNICK, Stuart; NETO, Nelson Novais; BORGES, Natasha Malara; PAULA, Anchises Moraes G. de. **Developing a Global Data Breach Database and the Challenges Encountered.** Association for computing machine. Digital Library. 15/01/2021 Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873

MANTUSO, Marcela; MENDES, Laura Schertel. **Discriminação algorítmica: Conceito, fundamento legal e Tipologia**. Proteção de dados e inteligência artificial: Perspectivas éticas e regulatórias. Porto Alegre. Dezembro/2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019

MARTINS, Guilherme Magalhães. **A lei Geral de Proteção de Dados Pessoais (LEI 13.709/2018) e a sua principiologia.** Revista dos Tribunais Online. Thomsom Reuters, Vol. 1027/2021. P 203 -243. Maio de 2021

MAYER-SCHÖNBERGER, Victor; CUKIER, Kenneth. **Big Data; The essential Guide to Work, Life and Learning in the Age of Insight**. 2017. Kindle

MAYOR OF LONDON, **Equality Impact Assessment (EqIA) for London Plan Guidance**. Disponível em: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.london.gov.uk/sites/default/files/public_london_charter_lpg_eqia.pdf

MAYOR OF LONDON. **High Street Data Service and Partnership.** Disponível em: https://data.london.gov.uk/high-street-data-service/ Acesso em 21/03/2023

MAYOR OF LONDON. **London Datastore.** Disponível em: https://data.london.gov.uk/?_gl=1%2a17r8k54%2a_ga%2aNDA4NzczMTUuMTY3ODg3NjIzNA..%2a_ga_PY4SWZN1RJ%2aMTY3OTM4OTEwMy4xLjAuMTY3OTM4OTEwMy42MC4wLjA. Acesso em 21/03/2023

MAYOR OF LONDON. **London Plan Guidance.** 2021. Disponível em: *https://www.london.gov.uk/programmes-strategies/planning/implementing-london-plan/london-plan-guidance*

MAYOR OF LONDON. **MD2861 London Plan Guidance**. 16/09/2021. Disponível em: https://www.london.gov.uk/decisions/md2861-london-plan-guidance

MAYOR OF LONDON. **Public London Charter.** Disponível em: https://www.london.gov.uk/programmes-strategies/planning/implementing-london-plan/london-plan-guidance/public-london-charter

MAYOR OF LONDON. **The London Datastore offer**. https://data.london.gov.uk/borough-partnership/the-london-datastore-offer/

MAYOR OF LONDON. **The London Plan.** Disponível em: https://www.london.gov.uk/sites/default/files/the_london_plan_2021.pdf

MICROSOFT. **O que é phishing?** Diponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-phishing

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS. **Conceito de Solução da Tecnologia da Informação e Comunicação. Governo Digital**. Última atualização 29/12/2022. Disponível em. https://www.gov.br/governodigital/pt-br/contratacoes/conceito-de-solucao-de-tic

MINISTÉRIO DA SAÚDE. **Registros de Incidentes com dados pessoais.** Disponível em*:* https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais

MOBICASCAIS. **App MobiCascais**. Disponível em https://mobi.cascais.pt/

MOBICASCAIS. **Serviços MOBI. Veículo autônomo** Disponível em https://mobi.cascais.pt/servicos/veiculoautonomo

MORAES, Alexandre de; HAYASHI, Vitor Takashi. **Segurança em IoT. Entendendo os riscos e ameaças em Internet das Coisas**. Editora Alta Books. 2021

MUKAI, Toshio. **Direito e legislação urbanística no Brasil.** Editora Saraiva. São Paulo. 1988

NISSA, Rob Kitchin. **The Real-Time City? Big Data and Smart Urbanism.** National University of Ireland Maynooth. Country Kildare, Irland. June 2013.

NORDIC SMART CITY NETWORK. **Smart city update from Tampere: Improving health care and heightening public safety.** Disponível em: https://nscn.eu/cityupdate/Tampere/healthandsafety

OLIVEIRA, Rafael Carvalho Rezende. **Curso de Direito Administrativo**. 6ª edição. Editora Método. 2018

ONE TRUST DATAGUIDANCE. *Greece.* **HDPA fines Cosmote £6M for data breach and unlawful data processing**. Regulation Research software. 01/02/2022**.** https://www.dataguidance.com/news/greece-hdpa-fines-cosmote-6m-data-breach-and-unlawful

O NEIL, Cathy. **Personality Tests Are Failing American Workers**. Bloomberg. 18/01/2018. Disponível em: https://www.bloomberg.com/view/articles/2018-01-18/personality-tests-are-failing-american-workers

OPEN & AGILE SMART CITIES & COMMUNITIES. Disponível em: https://oascities.org/

OSLO CITY BIKE. **Good for you, good for Oslo!** Disponível em: https://oslobysykkel.no/en

PANDYA, Sharnil; SRIVASTAVA, Gautan; JHAVERI, Rutvij e outros. **Federal Learning for smart cities: A comprehensive survey.** Sustainable Energy Technologies and Assessments. Elsevier. 2022.Disponível em: http://www.elsevier.com/locate/seta

PARENTONI, Leonardo Netto. **Compartilhamento de dados pessoais e a Figura do Controlador (Personal Data Sharing and the role of the Data Controller)** Abril 2021. Disponível em: < https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller>

PARENTONI, Leonardo Netto. LIMA, Henrique Cunha Souza. **Proteção de dados pessoais no Brasil: Antinomias Internas e Aspectos Internacionais.** Disponível em: https://www.researchgate.net/publication/340005766_Protecao_de_Dados_Pessoais_no_Brasil_Antinomias_Internas_e_Aspectos_Internacionais

PARENTONI, Leonardo Netto. **What Should We Reasonably Expect from Artificial Intelligence?** Julho de 2022. Disponível em: https://www.researchgate.net/publication/361988480_What_should_we_reasonably_expect_from_artificial_intelligence

PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Basic Anonymisation.** Disponível em: https://www.pdpc.gov.sg/Help-and-Resources/2018/01/Basic-Anonymisation

PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Basic Anonymisation Tool Now Available.** Disponível em: https://www.pdpc.gov.sg/News-and-Events/Announcements/2022/05/Data-Anonymisation-Tool-Now-Available

PERSONAL DATA PROTECTION COMMISSION SINGAPORE – **E-Learning Programme.** Disponível em: https://www.pdpc.gov.sg/Help-and-Resources/2018/01/E-Learning-Programme

PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Basic Anonymisation.** Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf

PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **PDPC's Advisory Guidelines on the Personal Data Protection Act for Selected Topics** Disponível em: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-selected-topics

PERSONAL DATA PROTECTION COMMISSION SINGAPORE – **Who we are.** Disponível em: https://www.pdpc.gov.sg/Who-We-Are/About-Us

POLÍCIA FEDERAL. **Polícia Federal deflagra Operação Deepwater que combate a obtenção e vazamento ilegal de dados pessoais de brasileiros pela internet**. 29/03/2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/03/policia-federal-deflagra-a-operacao-deepwater-que-combate-a-obtencao-e-vazamento-ilegal-de-dados-pessoais-de-brasileiros-pela-internet

PORTAL DE NOTÍCIAS DA GLOBO. **Google é multado nos EUA por coleta de dados pessoas para Street View.** https://g1.globo.com/tecnologia/noticia/2013/03/google-e-multado-nos-eua-por-coleta-de-dados-pessoais-para-street-view-2.html 12/03/2013.

PORTAL DE NOTÍCIAS DA GLOBO. **Hacker preso por mega vazamento de dados tem 24 anos e vive em Uberlândia; ele também é suspeito de invadir o Senado, o Exército e o TSE.** Disponível em: https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/19/suspeito-do-maior-vazamento-de-dados-do-brasil-e-preso-em-uberlandia.ghtml

PRARAHAJ, Sarbeswar; HAN, Hoon. **City, Culture e Society. Cutting through the clutter of smart city definitions: A reading into the smart city perceptions in India**. Vol. 18. September 2019. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1877916618302935

PREFEITURA DE SÃO PAULO. **Prefeito assina contrato para o início do Smar tampa, maior programa de videomonitoramento da cidade com até 40 mil câmeras.** Cidade de São Paulo. 07/08/2023. Disponível em*:* https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2

PRIVACY APP. **Welcome to PrivacyApp!** Disponível em: https://www.privacyapp.info/

PÚBLICO. **Hospital do Barreiro contesta judicialmente coima de 400 mil euros de Comissão de Dados.** 22/10/2018. Disponível em: https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479

QUEIROZ, Renata Capriolli Zocatelli, **Encarregado de Proteção de Dados Pessoais- DPO. Regulamentação e Responsabilidade Civil.** Editora Quartier Latin do Brasil. 2022

RANKING CONNECTED SMART CITIES. **Sobre o Ranking Connected Smart Cities**, Disponível em: https://ranking.connectedsmartcities.com.br

REPUBLIC OF BULGARIA. **Commission for Personal Data Protection. Information about CPDP's actions in relation to the personal data protection security breach at the National Revenue Agency.** 21/08/2019. Disponível em: https://www.cpdp.bg/en/index.php?p=news_view&aid=1505

REPUBLIC OF BULGARIA. **Commission for Personal Data Protection. Update on the undertaken inspetion at the National Revenue Agency.** 29/08/2019. Disponível em: https://www.cpdp.bg/en/?p=news_view&aid=1519

RODOTÁ, Stefano. **A vida na sociedade de vigilância. A privacidade hoje**. Editora Renovar. 2008.

RODRIGUES, Arlete Moysés. **Estatuto da Cidade: função social da cidade e da propriedade. Alguns aspectos sobre a população urbana e espaço**. Caderno Metrópole. Nº 12. 2 sem. 2004. 9-25 p.

ROLNIK, Raquel. **O que é cidade.** Editora brasiliense. 3ª edição. 1994

ROSENVALD, Nelson; DIAS, Daniel; FORTES, Pedro; VENTURI, Thais G. Pascoaloto. **Plataformas digitais e a (in)segurança de dados: O cerco ao TikTok**. MIGALHAS. 24/04/2023. Disponível em: https://www.migalhas.com.br/coluna/direito-privado-no-common-law/385252/plataformas-digitais-e-a-in-seguranca-de-dados-o-cerco-ao-tiktok

SAGE. **AI @ the edge for**. Disponível em: https://sagecontinuum.org/

SAID, Alan; TORRA, Vicenç. **Data Science in Practice.** Studies in Big Data. 46. Ed. Springer. 2018

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016

SÉGUIN, Elida. **Estatuto da cidade**. Editora Forense. Rio de Janeiro. 2002

SEWARD, Zachary M; DATOO, Siraj. **City of London halts recycling bins tracking phones of passers-by.** QUARTZ. 12/08/2013. Disponível em*:* https://qz.com/114174/city-of-london-halts-recycling-bins-tracking-phones-of-passers-by Acesso em 05/05/2023

SHARIF, Al Sharif; POKHAREL, Shaligram. **Engineering Advance. Smart City Dimensions and Associated Risks**. Sustainable Cities and Society (SCS) international journal. ScienceDirect Disponível em: https://www.sciencedirect.com/journal/sustainable-cities-and-society

SHEPARDSON, David; AYYUB, Rami. **TikTok congressional hearing: CEO Shou Zi Chew grilled by US lawmakers**. REUTERS. 24/03/2023. Disponível em: https://www.reuters.com/technology/tiktok-ceo-face-tough-questions-support-us-ban-grows-2023-03-23/

SILVA, Maria Fernanda; OLIVEIRA, Cristina Godoy Bernardo de. **O impacto social causado pelo uso de algoritmos discriminatórios e a superveniência da LGPD.** Migalhas. 04/11/2022 Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/376497/o-impacto-social-causado-pelo-uso-de-algoritmos-discriminatorios

SINGAPURE. **Smart Nation. Assistive Technology and Robotics In Healthcare. Improve Healthcare with Tech.** Disponível em*:* https://www.smartnation.gov.sg/initiatives/health/assistive-techonology-robotics

SINGAPURE. **Digital Readiness Blueprint.** Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mci.gov.sg/files/dr%20blueprint.pdf

SINGAPURE. **Smart Nation. Apps for you**. Disponível em https://www.smartnation.gov.sg/community/apps-for-you/

SINGAPURE. **Your Health at Your Fingertips.** Disponível em: https://www.smartnation.gov.sg/initiatives/health/healthhub

SOUZA, Carlos Affonso Pereira; LEMOS, Ronaldo. **Aspectos jurídicos da economia do compartilhamento: função social e tutela da confiança**. Vol. 08. Revista de Direito da Cidade

SOUZA, Carlos Afonso; LEMOS, Ronaldo. **Marco Civil da Internet. Construção e aplicação.** Editar Editora associada. 2016. Juiz de Fora- MG

TAMPERE. **SURE! Tampere. New ways to keep you secure.** Disponível em: https://suretampere.fi/

TAMPERE. **Urban security model developed in Tampere scales up in other European cities.** 06/07/2022. Disponível em: https://suretampere.fi/urban-security-model-developed-in-tampere-scales-up-in-other-european-cities/

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Thomson Reuters Brasil Conteúdo e Tecnologia LTDA. São Paulo. 2019.

THE EUROPEAN INSTITUTE FOR INNOVATION THROUGH HEALTH DATA. **Trustworthy Health ICT Systems**. Disponível *em:* https://www.i-hd.eu/trustworthy-health-ict-systems/

TIBCO. **O que são dados estruturados?** Disponível em: https://www.tibco.com/pt-br/reference-center/what-is-unstructured-data#:~:text=Dados%20n%C3%A3o%20estruturados%20s%C3%A3o%20dados,banco%20de%20dados%20relacional%20convencional.

TIKTOK. **Privacidade e segurança no TikTok**. Disponível em: https://www.tiktok.com/safety/pt-br/privacy-and-security-on-tiktok/

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. **TJSP mantém proibição de coleta de dados pela Via Quatro.** 10/05/2023. Disponível em**:** https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=91605&pagina=1

TUNGGAL, Abi Tyas. **What is Social Engineering? Definition + Attack Examples**. Up Guard. 06/04/2023. Disponível em: https://www.upguard.com/blog/social-engineering.

UNIÃO EUROPEIA. **A Autoridade Europeia para a Proteção de Dados.** Disponível em: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/edps_pt

UNIÃO EUROPEIA. ***European Data Protection Board. Guideline nº 07/2020: on the concepts of controller and processor in the GDPR.*** Brussels: 02 Sep. 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_pt>

UNIÃO EUROPEIA. **General Data Protection Regulation**. Disponível em https://gdpr-info.eu/

UNITED KINGDOM. **Guidance Surveillance Camera Commissioner's Code of Pratice**. Disponível em: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

UNITED KINGTOM. **Regulation of Investigatory Powers Act 2000**. Part 1. Chapter I, Interception warrants, Section 8. Disponível em: https://www.legislation.gov.uk/ukpga/2000/23/section/8/enacte

UNITED KINGDOM PARLIAMENT. **Research Briefing, Smart Cities**. 22/09/2021. Disponível em: https://post.parliament.uk/research-briefings/post-pn-0656/

UNITED STATES COURT. **What does the Fourth Amendment Mean?** Disponível em: https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0#:~:text=The%20Constitution%2C%20through%20the%20Fourth,deemed%20unreasonable%20under%20the%20law.

UNITED STATES OF AMERICA Supreme Court of the United States. **CARPENTER v. UNITED STATES.** Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

UNITED STATES OF AMERICA United States Court of Appeals for de Sixth Circuit. **About the Court.** Disponível em: https://www.ca6.uscourts.gov/about-court

UNITED STATES OF AMERICA. **US Code. Stored Communications act .** Title 18. Part 1. Chapter 121 §2701 Disponível em: https://uscode.house.gov/view.xhtml?req=(title:18%20section:2701%20edition:prelim

UNITED NATIONS. **Universal Declaration of Human Rights** – *Portuguese*. 1948 Disponível em https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por

VAZ, Bruna; ZOMBARDI, José Lucas; GUEIROS, Pedro. **O caso "Google x Marielle Franco" e a quebra do sigilo telemático genérica.** Consultor jurídico. 26/10/2023. Disponível em: https://www.conjur.com.br/2023-out-26/opiniao-google-marielle-franco-quebra-sigilo-telematico-generica/#:~:text=Para%20melhor%20compreens%C3%A3o%2C%20a%20quebra,de%20crime%2C%20mediante%20autoriza%C3%A7%C3%A3o%20judicial.

VIVES, Antoni. **Smart city Barcelona: The Catalan quest to improve future urban living**. Brighton. Sussex Academic Press, 2018

VORAKULPIPAT, CHALEE; KO, RYAN K. L; LI, QI, MEDDAHI, Ahmed. **Security and privacy in Smart City.** August 2021. HINDAWY. Security e communication Networks. Disponível em: https://www.hindawi.com/journals/scn/2021/9830547/

WAGGLE. **Access Waggle sensors**. Disponível em: https://docs.waggle-edge.ai/docs/tutorials/access-waggle-sensors

WAGGLE AI. **Scientific AI at the edge**. Disponível em: https://wa8.gl/

WYLIE, Bianca. **Civic Tech: A listo of questions we'd like Sidewalk plan for ist Toronto Project.** 30/10/2017. Torontoist. Disponível em: https://torontoist.com/2017/10/civic-tech-list-questions-wed-like-sidewalk-labs-answer/

ZIEGLER, Sébastien**. Internet of Things Security and Data Protection.** Springer. 2019

ZIOSI, Marta; HEWIT, Benjamin; JUNEJA, Prathm e outros. *Smart Cities:* **Reviewing the Debate about their Ethical Implications**. 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001761

ZUBOFF, Shoshana, **A era do capitalismo de vigilância. A luta por um future humano na nova fronteira do poder.** Editora Intrínseca LTDA. 1ª edição digital. 2021