Instituto Serzedello Corrêa
Centro de Formação, Treinamento e Aperfeiçoamento
Câmara dos Deputados
Instituto Legislativo Brasileiro
Senado Federal

Análise *Ex Ante* do Plano Nacional de Internet das Coisas (IoT):

Ambiente Cidades Inteligentes

Flávia Lacerda

Prof. MSc. Paulo Roberto Simão Bijos

Coletânea de Pós-Graduação, v.5, n.1
Políticas Públicas

TCU TRIBUNAL DE CONTAS DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

José Mucio Monteiro (Presidente)

Ana Arraes (Vice-presidente)

Walton Alencar Rodrigues

Benjamin Zymler

Augusto Nardes

Aroldo Cedraz de Oliveira

Raimundo Carreiro

Bruno Dantas

Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti

Marcos Bemquerer Costa

André Luís de Carvalho

Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Cristina Machado da Costa e Silva (Procuradora-Geral)

Lucas Rocha Furtado (Subprocurador-geral)

Paulo Soares Bugarin (Subprocurador-geral)

Marinus Eduardo de Vries Marsico (Procurador)

Júlio Marcelo de Oliveira (Procurador)

Sérgio Ricardo Costa Caribé (Procurador)

Rodrigo Medeiros de Lima (Procurador)

Análise *Ex Ante* do Plano Nacional de Internet das Coisas (IoT):
Ambiente Cidades Inteligentes

Flávia Lacerda

Monografia de conclusão de curso submetida ao Instituto Serzedello Corrêa do Tribunal de Contas da União como requisito parcial para a obtenção do grau de especialista.

Orientador(a):
Prof. MSc Paulo Roberto Simão Bijos

Banca examinadora:
Prof. Dr. Fernando de Barros Filgueiras

Brasília | 2020

REFERÊNCIA BIBLIOGRÁFICA

LACERDA, Flávia. **Análise *Ex Ante* do Plano Nacional de Internet das Coisas (IoT):** Ambiente Cidades Inteligentes. 2020. Monografia (Especialização em Avaliação de Políticas Públicas) – Instituto Serzedello Corrêa, Escola Superior do Tribunal de Contas da União, Brasília DF. 119 fl.

CESSÃO DE DIREITOS

NOME DO(A) AUTOR(A): Flávia Lacerda
TÍTULO: Análise *Ex Ante* do Plano Nacional de Internet das Coisas (IoT): Ambiente Cidades Inteligentes
GRAU/ANO: Especialista/2020

Flávia Lacerda
flavia.lacerda@tcu.gov.br

FICHA CATALOGRÁFICA

L131a Lacerda, Flávia

Análise *Ex Ante* do Plano Nacional de Internet das Coisas (IoT): Ambiente Cidades Inteligentes/ Flávia Lacerda. – Brasília: ISC/TCU, 2020.
119 fl. (Monografia de Especialização)

1. Avaliação de Políticas Públicas. 2. Internet das coisas. 3. Análise ex ante. 4. Privacidade. 5. Cidades inteligentes. I. Título.

CDU 02
CDD 020

Análise *Ex Ante* do Plano Nacional de Internet das Coisas (IoT): Ambiente Cidades Inteligentes

Flávia Lacerda

Trabalho de conclusão do curso de pós-graduação lato sensu em Avaliação de Políticas Públicas realizado pelo Instituto Serzedello Corrêa como requisito para a obtenção do título de especialista.

Brasília, 17 de julho de 2020.

Banca Examinadora:

_____
Prof. MSc. Paulo Roberto Simão Bijos
Orientador
Câmara dos Deputados

_____
Prof. Dr. Fernando de Barros Filgueiras
Avaliador
Fundação Getúlio Vargas

Dedico o trabalho aos meus amores, Victor e Arthur.

Agradecimentos

Agradeço a todos aqueles que contribuíram, de forma direta ou indireta, para a realização deste trabalho.

Aos queridos amigos Alexandre Peixoto e Fabiana Ruas, que me incentivaram (ou não) a encarar mais um desafio acadêmico; e Wesley Vaz, pelas ideias e discussões.

Aos companheiros de caminhada, Rommel Brandão, Fernanda Fiuza, João Ricardo, João Vicente e Leandro Teles, pela parceria durante e depois das aulas.

Ao chefe Fábio Granja e ao ex (eterno) chefe, Paulo André, pelo apoio de sempre.

Aos queridos amigos do ISC, em especial Clemens Santos, Cleuves Oliveira e Carol Dytz, por segurarem as pontas nas minhas ausências.

Aos coordenadores e professores da pós-graduação, especialmente Pedro Paulo e Renata Miranda, por todo o empenho para garantir a qualidade do curso.

Ao André Gomyde, pelas valiosas contribuições.

Ao prof. Paulo Bijos, pela orientação do trabalho, pela disponibilidade e pelas ideias compartilhadas.

Ao prof. Fernando Filgueiras, por gentilmente aceitar o convite para avaliar o trabalho.

“[Sicinius]
What is the city but the people?

[Citizens]
True,
The people are the city”.

(William Shakespeare,
Coriolanus: Act 3, Scene 1)

Resumo

Realiza-se análise *ex ante* do Plano Nacional de Internet das Coisas (IoT) e seus impactos para o desenvolvimento das cidades inteligentes no Brasil, com enfoque nas questões relacionadas à privacidade e proteção de dados dos cidadãos, no escopo das soluções de mobilidade urbana, segurança pública e eficiência energética propostas nos projetos-piloto da política. Apresenta-se um diagnóstico, com causas e evidências de problemas urbanos, como congestionamentos, violência nas cidades e consumo de energia elétrica no Brasil, e as propostas de soluções com o uso de tecnologias de IoT. Enumeram-se políticas nacionais e internacionais similares, em andamento ou finalizadas, bem como as razões para intervenção do Estado. Examinam-se dados sobre o impacto orçamentário e financeiro da política. Descreve-se a estrutura de governança adotada, com os principais atores envolvidos. Realiza-se análise crítica a partir de oito componentes do modelo de governança de políticas públicas do TCU, dentre os quais: institucionalização; planos e objetivos; participação; capacidade organizacional e recursos; coordenação e coerência; monitoramento e avaliação; gestão de riscos e controle interno; e *accountability*. Por fim, propõe-se a adoção de princípios para garantir uma abordagem mais sistêmica para a política pública de cidades inteligentes voltada para as necessidades dos cidadãos.

Palavras-chave: avaliação de políticas públicas; análise ex ante; internet das coisas; cidades inteligentes; privacidade.

Abstract

Ex ante analysis of the National Internet of Things (IoT) Plan and its impacts for the development of smart cities in Brazil, focusing on issues related to citizens' privacy and data protection, within the scope of urban mobility solutions, public security and energy efficiency proposed in the policy's pilot projects. Presents a diagnosis with causes and evidence of urban problems, such as traffic jam, violence in cities and consumption of electricity in Brazil, and proposals for solutions using IoT technologies. Specifies similar national and international policies in progress or finished, as well as the reasons for State intervention. Examines data on the budgetary and financial impact of the policy. Describes the governance structure adopted, with main actors involved. Presents a critical analysis based on eight components of TCU's public policy governance model, including: institutionalization; plans and objectives; participation; organizational capacity and resources; coordination and coherence; monitoring and evaluation; risk management and internal control; and accountability. Finally, proposes adopting principles to ensure a more systemic approach to public policy on smart cities focused on the needs of citizens.

Keywords: public policies evaluation; ex ante analysis; internet of things; smart cities; privacy.

Lista de figuras

Lista de gráficos

Lista de quadros

Sumário

1. Introdução

A política pública analisada neste trabalho é o Plano Nacional de Internet das Coisas (IoT), instituído pelo Decreto nº 9.854, de 25 de junho de 2019 (BRASIL, 2019a). Insere-se como política de infraestrutura no Plano Plurianual (PPA) 2016-2019 (BRASIL, 2016), Programa temático 2025: "Comunicações para o Desenvolvimento, a Inclusão e a Democracia". O foco da análise está no Objetivo 1135: "Promover a inovação, o desenvolvimento tecnológico e a competitividade da indústria nacional de telecomunicações", particularmente na Iniciativa 064G: "Lançamento do Plano Nacional de M2M/Internet das Coisas". Conforme o PPA:

> Em um mundo onde cada vez mais as transações comerciais e pessoais utilizam as TICs para seu funcionamento, o domínio tecnológico e produtivo dos equipamentos e softwares que suportam as redes de telecomunicações passa a ser não só uma questão de segurança nacional. O desenvolvimento tecnológico nacional também se mostra necessário com a notável convergência tecnológica, na qual pessoas e objetos passam a se conectar em uma grande rede, criando um terreno fértil para que o setor de telecomunicações prospere. A denominada "Internet das coisas" ou "IoT – Internet of Things", considerada a nova tendência tecnológica, é um conceito em que a maioria dos objetos e aparelhos do cotidiano possam estar conectados à Internet, gerando uma demanda cada vez maior para a indústria nacional e estrangeira, o que impacta diretamente em nossa balança comercial (BRASIL, 2016).

A portaria MCTIC nº 1.122/2020 indica a continuidade da priorização do tema "Internet das Coisas" ao detalhar a atuação ministerial para o PPA 2020-2023. A área foi designada no normativo como tecnologia habilitadora, que "tem como objetivo contribuir para a base de inovação em produtos intensivos em conhecimento científico e tecnológico" (BRASIL, 2020).

O Plano Nacional de IoT (BRASIL, 2019a) é parte fundamental da Estratégia Brasileira para a Transformação Digital - E-Digital (BRASIL, 2018), e implica em amplo impacto para o desenvolvimento econômico e tecnológico do país. A proposta do plano foi subsidiada pelo estudo "Internet das Coisas: um plano de ação para o Brasil" (BNDES, 2017d), conduzido pelo consórcio McKinsey/Fundação CPqD/Pereira Neto Macedo, por encomenda do Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O estudo apresenta 76 ações para guiar políticas públicas para IoT até 2022, com prioridade para os ambientes: cidades, saúde, rural e indústria. O plano contempla temas horizontais que incluem formação de capital humano, fomento à

inovação e inserção internacional, infraestrutura de conectividade e interoperabilidade, além de regulação de segurança e privacidade.

Pretende-se com este trabalho compreender, sob múltiplas perspectivas, os objetivos, o desenho, as estratégias e os possíveis impactos da política pública de IoT no Brasil de modo geral, e particularmente aspectos do plano que tangenciam o ambiente priorizado “cidades”, ou “cidades inteligentes” (*smart cities*). Para tanto, serão mapeadas as inciativas que relacionam IoT e cidades inteligentes, e os benefícios e desafios que trazem aos cidadãos e à gestão pública. Dentre os desafios, serão exploradas com maior ênfase as questões regulatórias relacionados à privacidade e proteção de dados pessoais no ambiente urbano mediado pelas tecnologias da IoT.

2. Problema e justificativa

A escolha desta política pública para análise justifica-se pela importância e atualidade do tema Internet das Coisas e seus impactos, considerando a complexidade e multiplicidade de aspectos e atores envolvidos, particularmente no que diz respeito às cidades inteligentes. A temática apresenta alta probabilidade de fragmentação e sobreposição em políticas e programas correlatos, além de risco evidente descontinuidade das ações, dada atual conjuntura econômica e social do país.

O extraordinário potencial da Internet das Coisas (IoT) é o poder que confere aos objetos de uso cotidiano de capturar, processar, armazenar, transmitir e apresentar informações. Interligados em rede, os objetos são capazes de realizar ações de forma independente e gerar dados em quantidade e variedade exponenciais, como produto das interações. A IoT afeta a humanidade em diferentes escalas. Envolve desde objetos de uso comum interconectados, equipados com sensores e identificados por radiofrequência (RFID) – capazes de trocar informações entre si, com as pessoas ou com o ambiente - até cidades inteiras sendo projetadas de maneira totalmente conectada e automatizada (cidades inteligentes ou *smart cities*), que são o foco desta pesquisa (LACERDA, 2015[1]).

Do ponto de vista tecnológico, a IoT é “uma infraestrutura dinâmica global com capacidades de autoconfiguração, baseada em protocolos de comunicação padronizados e interoperáveis, onde “coisas” virtuais e físicas possuem identidades, atributos físicos e personalidades virtuais, usam interfaces inteligentes e estão integradas de maneira transparente à Rede” (IERC, 2012). A arquitetura da IoT baseia-se em quatro camadas tecnológicas integradas: (1) dispositivos; (2) rede; (3) suporte a serviços e aplicações; e (4) segurança da informação, e as soluções de IoT são caracterizadas por três pré-requisitos: (1) transferência de dados digitais entre sensores e atuadores; (2) conexão com uma rede externa; e (3) capacidade autônoma de processamento de dados (BNDES, 2017d).

[1] Trechos deste trabalho foram extraídos da tese da autora (LACERDA, 2015), com a referência devidamente indicada e no limite de 10% do conteúdo total. Samuelson (1994) considera aceitável o percentual de 30% de reutilização, quando os dados dos trabalhos anteriores forem importantes para a continuidade das pesquisas, que é o caso.

De acordo com a Cartilha de Cidades elaborada pelo BNDES (2018b), a aplicação de tecnologias de IoT em ambiente urbano tem o potencial de trazer uma série de benefícios aos cidadãos nas áreas de transporte, segurança, eficiência energética, entre outras, com soluções capazes de promover desenvolvimento econômico, sustentabilidade e qualidade de vida. É possível ainda utilizar a massa de dados gerada pelas aplicações para otimizar o planejamento e a gestão de políticas públicas para a própria cidade.

O problema é que a velocidade com a qual a tecnologia se difunde na vida das pessoas é maior do que a possibilidade de previsão de seus impactos, sejam positivos ou negativos. Os desafios emergentes do contexto da IoT são de natureza e proporções variadas – como inclusão digital, privacidade, usabilidade, consentimento, para citar alguns. O tema tem sido tratado como prioritário pelo setor público de diversos países, com programas de governo dedicados a identificar impactos e potenciais oportunidades trazidas pelas inovações (LACERDA, 2015).

Em termos de materialidade, a *International Data Corporation* (IDC, 2019) prevê que em 2025 haverá 41,6 bilhões de dispositivos IoT conectados, ou "coisas", gerando 79,4 zettabytes de dados. Para Porter e Heppelmann (2015), a IoT representa “a mudança mais substancial na produção de bens desde a Segunda Revolução Industrial”. Em escala global, o potencial econômico que a IoT pode trazer para as cidades é de US$ 1,6 trilhão em 2025. No Brasil, há uma previsão de ganhos da ordem de US$ 27 bilhões no mesmo período, com iniciativas de redução de custos com iluminação pública, monitoramento do tráfego em tempo real e redução da mortalidade pela violência, entre outras. Alguns municípios já apresentam experiências bem-sucedidas nesse sentido, parte delas listada na referida cartilha do BNDES (2018b).

Em termos de políticas públicas no país, percebe-se em uma primeira análise um complexo arcabouço de programas e iniciativas relacionados ao tema. O governo tem investido em iniciativas basilares, como as voltadas à infraestrutura tecnológica, mas, para alcançar o próximo patamar de desenvolvimento das cidades inteligentes, precisará enfrentar desafios tais como os relacionados à capacitação de pessoal, contratação pública, tratamento de dados e cooperação entre municípios (BNDES, 2018b). Para a Associação Brasileira de Internet das Coisas (ABINC), é fundamental:

> [...] adotar uma abordagem colaborativa e multissetorial para discussões sobre política de IoT. A IoT é uma área desafiadora para os formuladores de políticas, pois é um ambiente em rápido desenvolvimento e sua tecnologia abrange muitos setores e usos. Uma abordagem de governança colaborativa, que se baseie na experiência e no engajamento de uma ampla gama de partes interessadas, será necessária para desenvolver soluções eficazes e apropriadas. As políticas devem ter como objetivo promover a capacidade dos usuários de se conectarem, falarem, inovarem, compartilharem, escolherem e confiarem de uma maneira que promova a inovação e permita os direitos do usuário (ABINC, 2019).

A Secretaria de Infraestrutura Hídrica, de Comunicações e de Mineração (SeinfraCom) do TCU priorizou o tema como situação-problema a ser analisada, com o intuito de averiguar a "ausência de política pública, planejamento e incentivos estatais para o desenvolvimento da internet das coisas (IoT) no Brasil". Conforme consta da descrição da situação-problema:

> [...] a internet das coisas é a nova realidade tecnológica que permitirá trazer ganhos de produtividade e eficiência ao setor produtivo (agronegócio, indústria e serviços), bem como melhorar as condições de vida da população. No entanto, é necessário que o país tenha um ambiente favorável, do ponto de vista, de pesquisa, inovação, tributário, política pública e regulatório, entre outros, para a implantação dessa nova realidade tecnológica (BRASIL, 2019a).

Nesse sentido, a pesquisa se justifica pela busca de compreender esse cenário político e normativo, e avaliar o andamento das iniciativas do IoT voltadas para o ambiente "cidades inteligentes" à luz de um referencial capaz de estabelecer o nível de maturidade das políticas e programas de governo, visando assegurar o interesse público na implantação das tecnologias da IoT no país.

> Entende-se por políticas públicas o conjunto de programas ou ações governamentais necessárias e suficientes, integradas e articuladas para a provisão de bens ou serviços à sociedade, dotada de recursos orçamentários ou de recursos oriundos de renúncia de receitas e benefícios de natureza financeira e creditícia. (BRASIL, 2018, p. 13)

O trabalho pretende trazer como diferencial uma visão sistêmica da interrelação entre os principais programas e iniciativas de governo relativos ao tema Internet das Coisas, com enfoque no ambiente "cidades", bem como avaliar o cumprimento dos objetivos e das metas desse planejamento, de forma a subsidiar futuras ações de controle.

A opção pela análise *ex ante* se fundamenta na premissa de que o instrumento serve como guia para avaliar, *a priori,* se a ação governamental "responde a um problema bem delimitado e pertinente", "se há um objetivo claro de atuação do Estado

e se propõe um desenho que efetivamente possa ser alcançado” com vistas a otimizar a aplicação dos recursos públicos e atender às necessidades da sociedade (BRASIL, 2018). Considerando que a política já está em andamento, o intuito é buscar, no que for possível, oportunidades de aperfeiçoamento de seu desenho e implementação.

3. Objetivos

3.1. Objetivo geral

Realizar análise *ex ante* do Plano Nacional de Internet das Coisas (IoT) e seus impactos para o desenvolvimento da IoT no Brasil, no que tange ao ambiente “cidades inteligentes” e aos aspectos de privacidade e proteção de dados dos cidadãos.

3.2. Objetivos específicos

1. Realizar diagnóstico do problema: identificação, causas, evidências no Brasil; comparação internacional; razões para intervenção e políticas relacionadas;
2. Caracterizar a política: objetivos; ações e metas; resultados e impactos esperados;
3. Avaliar o desenho e a implementação da política: público-alvo, priorização e seleção de beneficiários; período de vigência; agentes envolvidos; instrumentos normativos; e impacto regulatório;
4. Verificar o impacto orçamentário e financeiro da política;
5. Analisar as estratégias de construção de confiança e suporte da política;
6. Examinar as estratégias de monitoramento, avaliação e controle da política;
7. Realizar a análise crítica da política.

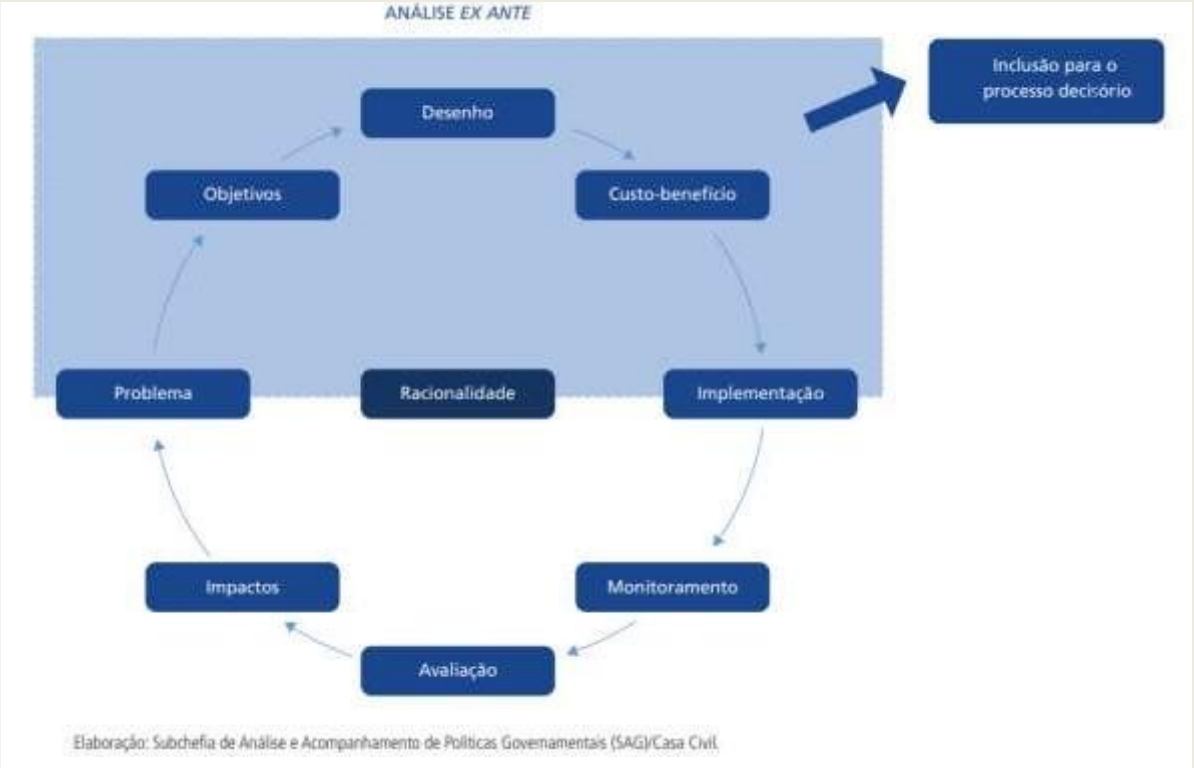
4. Metodologia

Adota-se a metodologia de pesquisa documental, exploratória, fundamentada em levantamento bibliográfico, com o objetivo de conhecer e analisar qualitativamente o objeto de estudo.

Utiliza-se como estrutura metodológica para o trabalho o documento “Avaliação de Políticas Públicas: Guia Prático de Análise *Ex Ante*” (2018), elaborado pela Casa Civil da Presidência da República e em parceria com o Ministério da Fazenda, o Ministério do Planejamento, Desenvolvimento e Gestão, o Ministério da Transparência e Controladoria-Geral da União (CGU) e o Instituto de Pesquisa Econômica Aplicada (Ipea).

O referido guia tem a finalidade de orientar a construção de políticas públicas com foco nas necessidades da sociedade e na melhoria do gasto público no Brasil. É usado para subsidiar a criação, expansão ou aperfeiçoamento das políticas, de forma a contemplar as etapas do ciclo de política pública ilustradas abaixo, buscando racionalidade, robustez e tempestividade da ação governamental. As seções seguintes detalham as etapas da análise *ex ante* do objeto de estudo deste trabalho.

Figura 1: Racionalidade no ciclo de política pública



Fonte: Casa Civil da Presidência da República e Ipea (2018)

A opção pela análise *ex ante* de uma política pública que está em andamento é no sentido de buscar oportunidades de aperfeiçoamento do desenho e da implementação, considerando que se trata de uma política complexa, com múltiplas variáveis e atores envolvidos, além de uma série de possíveis desdobramentos em outras ações governamentais ou normativos a serem desenvolvidos, que de fato já estão em curso.

Para proceder à análise crítica dos aspectos de governança do Plano Nacional de IoT, será utilizado como base, em caráter complementar, o "Referencial para Avaliação de Governança em Políticas Públicas" do TCU (BRASIL, 2014) em seus oito componentes, quais sejam: institucionalização; planos e objetivos; participação; capacidade organizacional e recursos; coordenação e coerência; monitoramento e avaliação; gestão de riscos e controle interno; e *accountability*.

5. Análise *ex ante* do Plano Nacional de IoT: Cidades Inteligentes

5.1. Diagnóstico do problema

5.1.1. Problemas, causas e evidências no Brasil

O cenário da IoT é multifacetado e os desafios emergentes são de natureza e proporções variadas. Dada a complexidade do tema, o estudo do BNDES (2017d) que embasou a elaboração do Plano Nacional de IoT utilizou uma metodologia de priorização de problemas internacionalmente adotada, dividindo-os em verticais e horizontais, em função de diversos critérios e métricas, tais como: impacto econômico e socioambiental, fortalecimento da cadeia produtiva, questões de infraestrutura, eficiência das instituições e capacidade de mobilização governamental.

As quatro verticais priorizadas no país foram: I – cidades; II – saúde; III – rural; e IV – indústria. As quatro horizontais foram I - capital humano; II - inovação e inserção nacional; III - infraestrutura de conectividade e interoperabilidade; e IV - regulatório, segurança e privacidade. Este trabalho tem como recorte a vertical “cidades” e os aspectos desta que se relacionam com a horizontal “regulatório, segurança e privacidade”, com foco em privacidade, além de alguns desdobramentos transversais de maior relevância para o ambiente urbano.

Vertical: Cidades

Segundo o IBGE (2007), mais de 85% da população brasileira vive atualmente em cidades, uma média de 170 milhões de pessoas. Dez das vinte maiores regiões metropolitanas da América Latina são brasileiras. Entretanto, “o crescimento acelerado da população urbana não foi acompanhado de um planejamento urbano eficaz e trouxe grandes desafios para os seus habitantes”. Dessa forma, “a infraestrutura local não conseguiu absorver a crescente demanda por produtos, serviços e espaços de locomoção” (BNDES, 2017a, p. 7).

> Com mais pessoas vivendo nas cidades é certo que uma série de problemas surgirão, envolvendo questões ligadas à mobilidade urbana, segurança pública, saúde, sustentabilidade ambiental, infraestruturas de energia e de saneamento, aprofundamento da desigualdade social, entre outros. Como forma de enfrentamento a estes desafios os gestores públicos e empresas privadas tem analisado o emprego de políticas públicas ligadas à Tecnologia da Informação e Comunicação (TIC), trazendo à tona a ideia da Smart City ou simplesmente Cidade Inteligente. (KNOPIK, 2018, p. 8).

Nesse contexto, a IoT surge como instrumento para ampliar o potencial dos serviços públicos ofertados aos cidadãos. No estudo realizado pelo BNDES (2017d) , que compila diversas outras fontes, foram identificados dez eixos com os desafios e potenciais aplicações de IoT para solucioná-los. Dos dez, foram priorizados, em função do impacto, quatro eixos: mobilidade urbana, segurança pública, eficiência energética e saneamento, e saúde. Os três primeiros, ilustrados a seguir, referem-se mais diretamente aos problemas do ambiente cidades inteligentes, foco deste trabalho. (BNDES, 2017d).

Quadro 1: Cidades brasileiras: 10 eixos para IoT

Eixos	Exemplos de desafios	Potenciais aplicações de IoT[1]	
Mobilidade	▪ **Transporte público:** 3 das 50 cidades mais congestionadas do mundo são brasileiras.	▪ Temporização automática de semáforos com base nas condições do trânsito	**Mobilidade, segurança, eficiência energética e saneamento são as três aplicações com maior impacto de IoT**
Segurança publica	▪ **Incidentes:** o Brasil é 10º país mais violento do mundo, em termos relativos, e sua taxa de homicídios vem crescendo 4% ao ano.	▪ Sensores de detecção de sons de ocorrências ▪ Identificação de ocorrências por câmeras	
Eficiência energética e saneamento	▪ **Gestão e distribuição de recursos básicos:** iluminação pública consome cerca de 4% da energia elétrica do país, com um potencial de ganho de eficiência de 40%.	▪ Iluminação pública inteligente ▪ Medidores elétricos inteligentes	

Fonte: adaptado de BNDES (2017d)

Horizontal: Regulatório - privacidade

Além dos problemas específicos do ambiente urbano, é preciso analisar os desafios horizontais que afetam potencialmente todos os ambientes equipados com soluções de IoT. O quadro a seguir detalha as barreiras elencadas para cada horizontal priorizada pelo estudo do BNDES (2017d).

Quadro 2: Questões horizontais da IoT no Brasil

Horizontais	Barreiras
Capital humano	▪ Disparidade entre capacitação de gestores públicos e parceiros do setor privado para lidar com IoT. ▪ Capacitação de mão de obra para prototipagem de produtos no âmbito de cidades (p.ex., laboratórios de fábrica/*living labs* nos municípios).
Inovação e inserção internacional	▪ Baixos vínculos de prefeituras com *start-ups* e Instituições de Ciência e Tecnologia (ICTs) e falta de práticas de compartilhamento dos dados, que podem fomentar surgimento de novos negócios. ▪ Orçamentos municipais não comportam grandes investimentos em IoT e, portanto, são necessários outros modos de financiamento, como parcerias público-privadas, empréstimos de bancos de desenvolvimento e transferências voluntárias de outras esferas. ▪ Municípios de pequeno porte ainda enfrentam dificuldades para estabelecer parcerias público-privadas. ▪ Baixa cooperação horizontal de regiões metropolitanas, evidenciada pela existência de consórcios intermunicipais pontuais. ▪ Falta de integração e articulação administrativa das secretarias e demais órgãos públicos municipais.
Infraestrutura de conectividade e interoperabilidade	▪ Deficiências em infraestrutura básica de conectividade em determinados municípios.
Ambiente regulatório	▪ Barreiras regulatórias para uso de dados públicos dos cidadãos. ▪ Barreiras regulatórias existentes em *smart grid*, como a lógica de incentivos regulatórios para investimento e a regulamentação de tarifas inteligentes, que estão sendo endereçadas pela ANEEL. ▪ Contratos de prestação de serviços baseados em processo e não em resultado inibem a implantação de IoT. ▪ A legislação de compras públicas impõe alta complexidade e por vezes inviabiliza contratação de soluções tecnológicas.

Fonte: BNDES (2017d), destaque da autora

Neste trabalho optou-se pelo enfoque na horizontal ambiente regulatório, particularmente nos aspectos relacionados à privacidade dos dados dos cidadãos, no que tange às aplicações da vertical cidades selecionadas para análise (mobilidade, segurança pública e eficiência energética), conforme destacado no quadro acima.

Dados constituem a essência da Internet das Coisas. Debates sobre o direito aos dados produzidos e utilizados no âmbito da IoT têm sido pauta frequente dos mais diversos fóruns na área. Surgem questões como: a quem caberá decidir sobre que

dados serão abertos, restritos ou sigilosos – ao próprio usuário, ao governo, às empresas proprietárias das soluções? (MCEWEN; CASSIMALLY, 2013). Até que ponto a infraestrutura das cidades inteligentes garantirá aos cidadãos o acesso e o direito aos dados por eles gerados nas atividades cotidianas? (GREENFIELD; KIM, 2013). Informações de prontuário médico, por exemplo, poderão ser interligadas em rede e utilizadas para as mais variadas finalidades? (MCEWEN; CASSIMALLY, 2013). E quanto ao "direito a ser esquecido" em um cenário de bilhões de objetos trocando dados relativos ao indivíduo? (SANTUCCI, 2014).

Os temas "segurança da informação" e "privacidade" foram discutidos no *Open Internet of Things Assembly*, que ocorreu em Londres em 2012. O evento tratou dos direitos do *data subject* (sujeito do dado) – indivíduo a quem os dados pertencem, independentemente de ser o proprietário dos sensores (*data licensor*) ou do local onde os dados foram coletados. Para McEwen e Cassimally (2013), ainda não há um entendimento claro sobre tais direitos, mas é obviamente necessária a atenção de atores das mais diversas esferas envolvidas com a IoT para questões como: quais os limites éticos e legais para o arquivamento, a análise, a mineração e a interpretação da massa de dados gerada no contexto da IoT pelas empresas, e em que medida esses dados podem ser compartilhados com outras empresas? Chegaremos ao ponto de admitir que a privacidade não é mais possível? Considerando situações práticas: ao visitar um lugar público com sensores e dispositivos que captam informações, quem será o detentor dos dados eventualmente coletados – o proprietário dos sensores?, questionam os atores (LACERDA, 2015).

Greenfield e Kim (2013) observam que "quase que por definição, cada ato na cidade inteligente é formalizado, cada comportamento é observado, e cada observação gera um registro. E cada registro estará disponível para consulta pelos administradores". E acrescentam: "a noção de que as cidades são máquinas com fluxos que podem ser otimizados, e a decisão sobre investimentos que garantam essa máxima eficiência em detrimento de outras finalidades deveria partir de um processo de decisão democrático – otimizar para alcançar que finalidades, e em benefício de quem?" (LACERDA, 2015).

Conforme descreve a Cartilha de Cidades do BNDES:

> A crescente utilização de dispositivos tecnológicos dispersos pelo espaço urbano, capazes de coletar dados sobre os cidadãos, monitorar suas atividades e até mesmo identificá-los, traz à tona diversas questões referentes à proteção da privacidade e dos dados pessoais dos indivíduos. Para que o planejamento público das cidades inteligentes seja uma realidade bem-sucedida, é imprescindível que a privacidade dos cidadãos seja garantida primeiro na implementação das cidades inteligentes (BNDES, 2018b, p. 43).

Um caso emblemático ocorrido no Brasil foi o da empresa responsável pela linha amarela do metrô de São Paulo, que instalou câmeras para coleta de dados faciais nas plataformas, para analisar a emoção dos passageiros. A justiça determinou a interrupção da coleta, que foi considerada ilegal, dado que não houve consentimento dos usuários (IDEC, 2018).

As cidades de São Francisco e Cambridge (EUA), ambas referências acadêmicas e de mercado na área de tecnologia, baniram a vigilância por técnicas de reconhecimento facial pelo poder público (POLLO, 2020). Outro fato simbólico foi a publicação de um manifesto - *Abolish the #TechToPrisonPipeline* (2020), por diversos pesquisadores e profissionais de áreas como estatística, inteligência artificial, direito, sociologia, história, comunicação e antropologia, em repúdio a pesquisas sobre tecnologia de previsão de crimes (ou tecnologia carceral), por “reproduzirem injustiças e causarem danos reais”. O estudo do BNDES (2017b) cita diversos outros exemplos de situações problemáticas envolvendo privacidade em cidades inteligentes.

O grupo de especialistas em Internet das Coisas instituído pela União Europeia - *IoT Expert Group,* publicou a seguinte afirmativa em seu relatório de conclusão: “Considerando que a IoT introduz novas dificuldades para a integridade contextual, há um princípio segundo o qual as informações fornecidas para o uso em um dado contexto [ex; uma consulta médica] não devem ser usadas em um contexto diferente [pelos seguros de saúde, por exemplo]”. Segundo o grupo, deverá haver um contrato social entre pessoas e objetos, cujas ramificações éticas precisam ser consideradas (EUROPEAN COMMISSION, 2012).

Todo avanço tecnológico disruptivo traz cargas de utopia e distopia. A industrialização produziu inúmeros benefícios, ao preço dos efeitos colaterais da poluição ambiental, por exemplo. Situação análoga ocorre na IoT: os riscos contra a privacidade não podem ser inteiramente evitados, mas podem ser mitigados (LUCAS; BALLAY; MCMANUS, 2012). Os mais pessimistas acreditam que “a tecnologia onipresente nos aprisiona”: a metáfora distópica implica em uma preocupação de que

a tecnologia seja utilizada como mecanismo de vigilância e limite a livre atuação dos cidadãos, uma vez que seus dados poderão estar em poder de governos, organizações e indivíduos, abrindo oportunidades para a criação de novas formas de tirania, observa Kuniavsky (2010).

O urbanista e crítico Adam Greenfield (2006) alerta para o fato de que a IoT deve ser cuidadosamente arquitetada no momento presente, pois trará cada vez mais implicações para a humanidade. Ressalta ainda a urgência de articulação de padrões essenciais para um desenvolvimento ético e responsável, considerando os impactos de uma "vida colonizada pela tecnologia da informação". O autor destaca o papel dos reguladores, considerando o claro potencial das tecnologias de prejudicar a privacidade e a condição do espaço público e de comprometer o exercício de liberdades civis: "a grande massa de pessoas expostas a essas tecnologias terá relativamente pouco a influir nessa composição – e terá sua realidade afetada e moldada de inúmeras formas pelo advento da informática ambiente, pervasiva e ubíqua" (LACERDA, 2015).

Greenfield e Kim (2013) citam o caso do Centro de Operações do Rio de Janeiro, implantado pela IBM, como representativo dessa abordagem. Em sua visão, o investimento de 14 milhões de dólares – que agrega, em uma sala ao estilo "cenário de guerra", dados de vigilância da cidade, patrulhamento policial, clima, tráfego de veículos, sensores de esgoto e postagens em redes sociais – serve aos propósitos dos administradores da cidade e do vendedor da solução, mas é questionável se considera realmente os direitos e interesses da população. Ressaltam ainda o perigo do exercício do autoritarismo de um Estado obcecado pela observação e controle dos processos urbanos, que passaria a enxergar os cidadãos como meros geradores de dados, com implícitas intenções de observar e controlar comportamentos humanos (GREENFIELD, 2006; GREENFIELD; KIM, 2013).

Na mesma linha, Mendes (2011) defende que tecnologias e mercados não podem existir independentemente de princípios abrangentes de um sistema ético e social. A IoT terá um amplo impacto em muitos dos processos que caracterizam a vida cotidiana, portanto, é primordial que seu desenvolvimento seja fundamentado em estratégias orientadas a pessoas. Para isso, aqueles que as projetam devem estar próximos aos que irão utilizá-las (LACERDA, 2015).

O grupo de especialistas da Comissão Europeia - *IoT Expert Group* (2012) identificou seis questões éticas fundamentais no âmbito da IoT: justiça social (combate

à exclusão digital e de conhecimentos); confiabilidade (garantia de privacidade e segurança, proteção de dados); clareza sobre contextos (responsabilidades dos atores no ecossistema, privado versus público); clareza sobre metáforas (conveniência versus perigos das “coisas inteligentes”); clareza sobre agência de objetos (contrato entre pessoas e objetos); e autonomia dos indivíduos (consentimento informado sobre funcionalidades e ações dos objetos) (LACERDA, 2015).

Em “City of Bits” (1996), William Mitchell, do MIT, repensava em termos de arquitetura e urbanismo o contexto da revolução digital, da miniaturização dos eletrônicos, da mercantilização dos bits, e da crescente dominação dos softwares sobre as formas materiais. Ele considerava como o maior desafio não a instrumentação tecnológica dos espaços nem a produção de conteúdos digitais; mas imaginar e criar ambientes digitalmente mediados em função da vida que gostaríamos de levar e do tipo de comunidades que queremos produzir. Afirmava que não devemos ser passivos diante da emergência de estruturas cívicas e arranjos espaciais na era digital – que são determinantes do acesso a oportunidades econômicas e serviços públicos, do discurso público, da atividade cultural, das relações de poder e das experiências que dão forma e textura ao nosso dia-a-dia. Para Mitchell (1996). “é importante compreender o contexto para buscar alternativas futuras, para que possamos interferir, algumas vezes resistir, organizar, legislar, planejar e projetar” (LACERDA, 2015).

Durante a palestra “*On Public Objets: Connected Things and Civic Responsibility”* (2010), Greenfield sugere a discussão do “urbanismo em rede”, destacando a crescente gama de objetos comuns e lugares na cidade que estão identificando-se a redes globais ou sendo por estas identificados. O autor alerta para o fato de que estarmos instrumentados por tecnologias traz benefícios óbvios, mas pode gerar insumos indesejáveis, como a captura de informações para o alcance de interesses comerciais. E cita o exemplo do monitoramento por sensores das estradas da Finlândia, que inegavelmente melhora o trânsito e os acidentes, constituindo-se em bem comum, em contraste com as máquinas de bebidas japonesa que criam inadvertidamente perfis automáticos dos consumidores para oferecer produtos “customizados”, numa tentativa enviesada de adivinhar as preferências (LACERDA, 2015).

Greenfield (2010) define “objeto público” como "qualquer objeto distinto no domínio espacial comum destinado ao uso e fruição do público em geral, independentemente da sua propriedade ou intenção original". E argumenta que os objetos públicos devem ser considerados “bens públicos”, e devem disponibilizar dados abertos por meio de APIs acessíveis a qualquer interessado, para leitura, e, se for o caso, escrita segura, com possibilidade de uso para outras finalidades. O autor conclui que é preciso “agir contra a captura de espaço público por interesses privados, em direção a uma esfera pública revitalizada” (LACERDA, 2015).

Em “*Against the Smart City”*, Greenfield e Kim (2013) tratam das “cidades inteligentes” desenvolvidas a partir do zero como precursoras e exemplos do tipo de ambiente urbano que habitaremos quando as cidades forem “decisivamente colonizadas pela tecnologia, em um futuro próximo”. Eles criticam a “ideia passiva de subjetividade urbana e cidadania” inscrita nas visões de cidades inteligentes em desenvolvimento, nas quais “opta-se por ocultar distinções significativas entre público e privado”, não deixando claros aos usuários, por exemplo, a origem e o destino das informações capturadas. Afirmam, por fim, que forças de mercado estão determinando os parâmetros dos empreendimentos, desconsiderando os especialistas, a história e as teorias do planejamento urbano. “Qual a proposição de valor embutida nessas cidades?”, questionam (LACERDA, 2015).

5.1.2. Comparação internacional

O referido estudo do BNDES para a implantação de IoT no Brasil incluiu um amplo *benchmark* de iniciativas e políticas públicas (BNDES, 2017c) para a compreensão dos estágios de evolução da IoT e as principais tendências em 12 países, com diferentes realidades sociais, econômicas e tecnológicas. A pesquisa foi utilizada como referência para a antecipação de desafios e a adoção de boas práticas. Em síntese, os pontos analisados e as respectivas conclusões foram:

a. Envolvimento do governo

Depende do contexto e objetivos do país.

(I) Papel ativo: investimentos, seleção de áreas prioritárias, criação de associações e alianças, regulação e parcerias internacionais, consolidação das ações em um plano nacional.

(II) Formador de ecossistema: cria ambiente propício e coordena atores (empresas, agências de fomento, startups, universidades).

(III) Elaborador de diretrizes e investidor: realiza investimentos, difunde melhores práticas e viabiliza competitividade e abertura de mercados.

b. Modelos de governança

Define papéis para iniciativa privada, academia e setor público.

(I) Modelo estruturado: associações específicas ou alianças de IoT formadas pelos setores público e privado: com conselhos executivos e consultivos, além de grupos de trabalho ou comitês temáticos. Adotado pelos países com papel ativo do governo em IoT.

(II) Formação de ecossistema: modelo mais descentralizado, com incubadoras e consórcio de universidades, ou ações de coordenação focadas em áreas selecionadas.

c. Estímulos a inovação

Concentra-se no incentivo à formação de ecossistemas, pesquisa e empreendedorismo, e na redução de riscos.

(I) Investimentos: significativos na maior parte dos governos líderes em IoT.

(II) Clusters: reunião de startups e empresas em áreas específicas para troca de experiências e realização de negócios.

(III) PMEs e startups: fomento ao empreendedorismo pela redução de burocracia e impostos, e incentivo pela comunicação.

(IV) Compras públicas: uso da demanda de inovações pelo setor público para promover a inovação.

d. Formação de capital humano

Vincula políticas públicas de aumento da capacidade do setor às oportunidades de emprego.

(I) Programadores mirins: habilidades programação desde o ensino fundamental.

(II) Universidade e indústria: ampliar canais de cooperação entre iniciativa privada e academia.

(III) Eventos: organização de workshops, conferências e treinamentos em tópicos específicos.

e. Regulamentação

Considerado fator crítico, mas ainda não há clareza nem consenso. Temas-chave:

(I) Padronização: alguns países estimulam padrões abertos, outros, a adoção de padrões globais ou definidos pelo mercado para interoperabilidade das soluções.

(II) Conectividade: alguns governos desenvolvem infraestrutura local (EU, JP, KR), outros estão buscando a formação de plataformas globais (UK, CH, SG).

(III) Privacidade e segurança: governos ainda têm avançado em ritmos diferentes na aprovação de leis e criação de instituições responsáveis pela aplicação, ainda que haja consenso sobre a relevância dos temas.

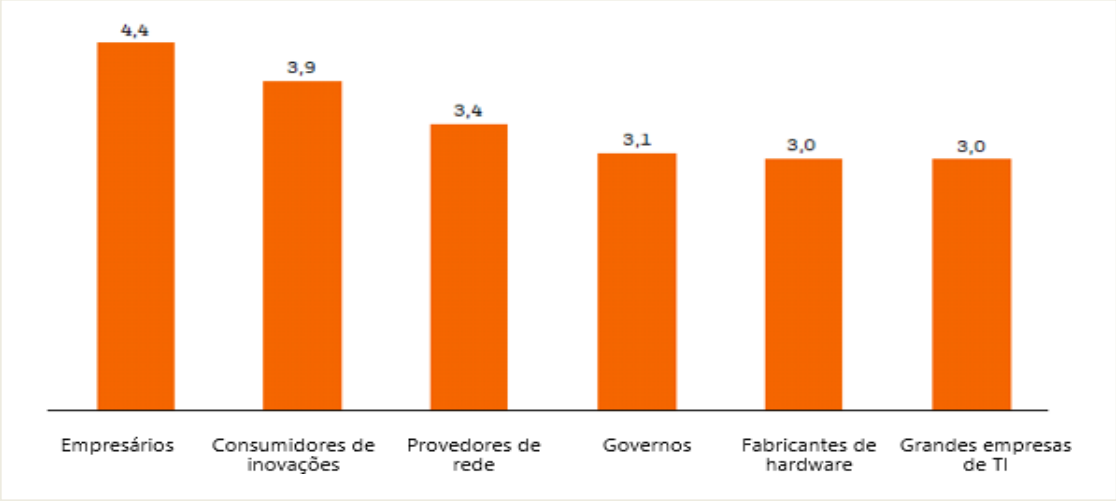
De acordo com o relatório, as regiões que se destacam na adoção de IoT são: União Europeia, Japão, Coreia do Sul, China, Estados Unidos, Reino Unido, Alemanha e Suécia. Em termos de importância do papel do Estado, sobressaem-se Cingapura e Emirados Árabes. Os países que apresentam maior similaridade de desafios com o Brasil são Índia e Rússia. (BNDES, 2017c). Iniciativas como *The Alliance for Internet of Things Innovation* (AIoTI), da União Européia e *Digital Catapult,* do Reino Unido, são exemplos de como o governo pode organizar e estimular a implementação de IoT nos países, aproveitando de forma mais eficiente o valor potencial das tecnologias. A imagem a seguir indica as aspirações e estratégias das regiões analisadas.

Figura 2: Aspirações e estratégias de IoT dos países selecionados

Fonte: BNDES (2017c)

Em um estudo anterior realizado pela *Fundación Bankinter Innovación* (2011) em parceria com a Accenture, que considerou respostas de mais de 400 especialistas, membros do *Future Trends Forum* (FTF), foram indicados os agentes direcionadores da adoção da IoT e seu respectivo grau de influência (escala: 1=insignificante, 5=muito importante) (LACERDA, 2015).

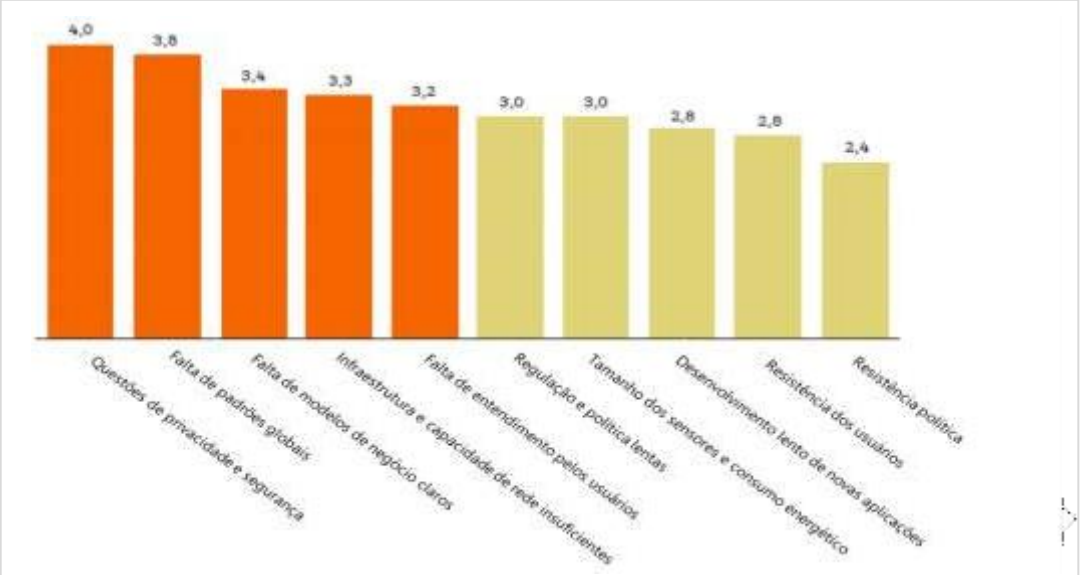
Gráfico 1: Agentes direcionadores da adoção da IoT



Fonte: adaptado de Fundación Bankinter Innovación (2011)

O gráfico a seguir, do mesmo estudo, ilustra sinteticamente alguns fatores que desafiam a adoção da IoT (escala: 1=insignificante, 5=muito importante.

Gráfico 2: Desafios para adoção de IoT



Fonte: adaptado de Fundación Bankinter Innovación (2011)

Em 2017 a União Internacional de Telcomunicações (UIT) elencou dez iniciativas de IoT relacionadas ao alcance dos Objetivos Desenvolvimento Sustentável - ODS (OBSERVATÓRIO DA TRANSFORMAÇÃO DIGITAL, 2018a):

1. Promover o desenvolvimento e a adoção de Tecnologias IoT em benefício da humanidade, do meio ambiente e do desenvolvimento sustentável […];
2. apoiar a implementação da IoT no contexto urbano e rural para promover a aplicação de Institutos de Ciência e Tecnologia (ICT) no fornecimento de serviços para criar cidades e comunidades mais inteligentes e mais sustentáveis […];
3. promover um ecossistema abrangente, dinâmico e seguro de IoT, incluindo suporte a startups e incubadoras […];
4. estimular o desenvolvimento e a implementação de padrões que facilitem a interoperabilidade entre tecnologias e soluções IoT para pavimentar o caminho para um ecossistema aberto e interoperável […];
5. adotar aplicações inovadoras de IoT para lidar com os desafios associados a fome, abastecimento de água e segurança alimentar […];
6. estimular o interesse no uso da IoT para redução de riscos e mitigação de mudanças climáticas […];
7. identificar e apoiar a tendência crescente de uso de tecnologias IoT na educação […];

8. adotar a aplicação e o uso da IoT na conservação da biodiversidade e no monitoramento ecológico […];
9. contribuir para a pesquisa global e discussões sobre IoT em cidades inteligentes e sustentáveis por meio de iniciativas globais […];
10. promover o diálogo e a cooperação internacional sobre a IoT no desenvolvimento sustentável […].

O Plano Nacional de IoT contempla 43% das metas dos ODS, conforme figura adiante.

Figura 3: Metas dos ODS contempladas pelo Plano Nacional de IoT

Fonte: Observatório da Transformação Digital (2018a)

Conforme descrito na E-Digital (2018a), as políticas públicas de IoT impactam diretamente os seguintes ODS:

- Objetivo 2 - Fome Zero: IoT aumento na produtividade na agropecuária e reduzir perdas no campo e na logística de transporte e distribuição.
- Objetivo 3 - Saúde e Bem-Estar: uso de terminais móveis com acesso a bases de dados médicas e viabilizando prontuários eletrônicos; e a Internet das Coisas, com monitoração e diagnóstico remoto.
- Objetivo 9 - Indústria, Inovação e Infraestrutura: ampliação da infraestrutura de acesso à Internet, empreendedorismo digital, e Internet das Coisas.

Particularmente no que se refere a políticas de cidades inteligentes, a figura a seguir ilustra os objetivos idealizados pelos Emirados Árabes, Índia e Estados Unidos.

Figura 4: Visões e objetivos para cidades inteligentes

Fonte: BNDES (2017c)

Em termos de critérios para seleção de projetos-piloto para fomento, Índia e Estados Unidos lançaram programas com as seguintes características:

Figura 5: Critérios de outros países para seleção de pilotos de cidades inteligentes

Fonte: BNDES (2017c)

A ilustração a seguir traz exemplos de aspirações de algumas das cidades norte-americanas para cidades inteligentes.

Figura 6: Aspirações para cidades inteligentes norte-americanas

Fonte: BNDES (2017c)

Por fim, o relatório de benchmarking realizado no âmbito do estudo do BNDES (2017c) elencou resumidamente as boas práticas identificadas no planejamento e seleção de pilotos para cidades inteligentes.

Quadro 3: Planejamento e seleção de pilotos de cidades inteligentes

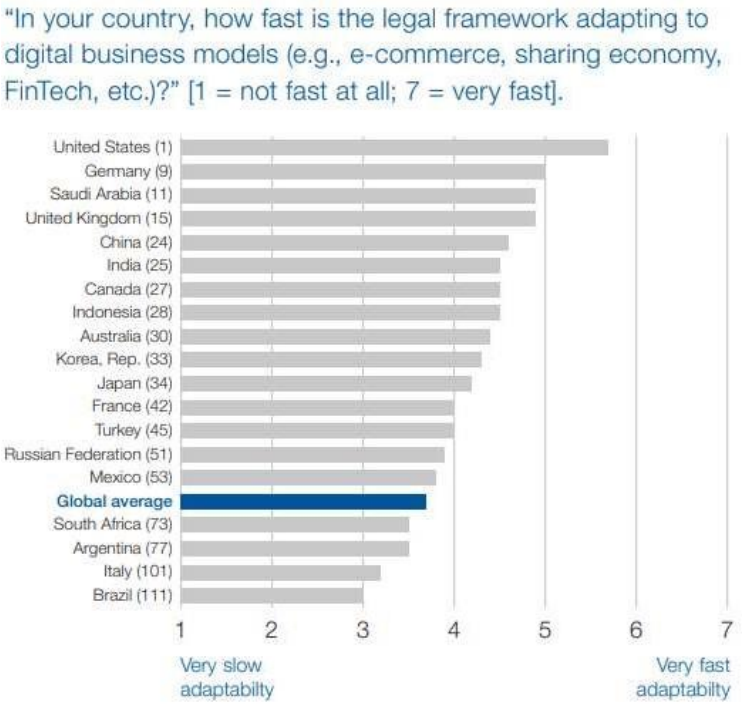
	Descrição
Abertura de editais de candidatura de cidades	• Forma mais comum de seleção de cidades, visto que é uma forma bastante direta de mensurar vontade política da gestão municipal para promover a transformação da cidade
Envolvimento do setor privado no planejamento e financiamento dos pilotos	• Fator relevante, visto que o investimento para transformação das cidades é relativamente alto, e, no contexto brasileiro, municípios e estados já enfrentam restrições orçamentárias importantes, além do apoio técnico aos municípios
Grande importância da visão e ambição das cidades	• Importante critério para seleção de apoio de pilotos em cidades específicas. O alinhamento dessa visão com o planejamento mais abrangente das cidades também denota o quão central é a utilização de IoT para a prosperidade do município, levando a Internet das Coisas a um patamar de instrumento chave
Avaliação do nível de replicação e escalabilidade dos pilotos	• Pontos fundamentais presentes em experiências internacionais pois ressaltam a importância da consolidação de aprendizados de um projeto específico e sua transposição para demais cidades que também apresentam desafios similares em IoT
Ampla participação da sociedade na escolha dos pilotos/áreas beneficiadas	• Requisito considerado indispensável por alguns programas e utilizado em conjunto com diagnóstico da cidade para priorizar aplicações de IoT

Fonte: BNDES (2017c)

5.1.3. Razões para intervenção

A realidade brasileira apresenta uma série desafios para a melhoria dos índices de competitividade e das condições de vida dos cidadãos. O crescimento econômico do país está abaixo de diversos países emergentes, e é alto o nível de insatisfação da população em relação aos serviços básicos oferecidos. Em 2013, o Brasil chegou a ocupar a 48ª posição no ranking de competitividade do Fórum Econômico Mundial. Atualmente está na 71ª. Um dos pontos avaliados no relatório é a adaptabilidade do arcabouço legal aos negócios digitais. Nesse quesito, o país está abaixo da média global, ocupando a 111ª posição de 141, conforme gráfico a seguir.

Figura 7: Governança tecnológica: adaptabilidade do arcabouço legal



Fonte: *World Economic Forum* (2019)

Além dos problemas recorrentes, novos desafios estão surgindo em função dos recentes avanços da tecnologia, como a automação no mercado de trabalho e a consequente necessidade de requalificação da mão-de-obra. No estudo do BNDES

(2017d) foi realizada análise da demanda por IoT no Brasil, e elencados os setores de maior impacto potencial, que definiram a aspiração do país em relação às tecnologias:

> Acelerar a implantação da Internet das Coisas como instrumento de desenvolvimento sustentável da sociedade brasileira, capaz de aumentar a competitividade da economia, fortalecer as cadeias produtivas nacionais, e promover a melhoria da qualidade de vida (BNDES, 2017d, p. 23 Relatório Final).

Os três macrodesafios identificados para o país na área são: (1) aumentar a produtividade e competitividade no mercado global; (2) expandir o acesso e a qualidade de serviços críticos – como saúde, mobilidade urbana e segurança – para melhoria do bem-estar e qualidade de vida; e (3) adequar perfis profissionais e relações de trabalho. (BNDES, 2017d). O segundo ponto é o que tem maior relação com o recorte feito para este trabalho. Na vertical “cidades” são feitas as intervenções que afetam diretamente a qualidade de vida das pessoas, como as relativas à mobilidade urbana e segurança pública.

A mobilidade nas metrópoles brasileiras está entre as piores do mundo, devido ao elevado tempo de deslocamento, que impacta inclusive o crescimento econômico do país, concentrado primordialmente nas grandes cidades. Os custos de congestionamento correspondem em média de 2% a 4% do PIB de diferentes países. Outro fator de insatisfação dos cidadãos é o alto índices de mortes no trânsito. Dados comparativos estão disponíveis no estudo do BNDES (2017d). Em termos de segurança pública, os dados do país são alarmantes: temos a 15ª maior taxa de homicídios do mundo (UNODC, 2019), e 10 das 50 cidades mais violentas do planeta são brasileiras (SEGURIDAD, JUSTICIA Y PAZ, 2019).

Um dos resultados almejados no planejamento estratégico para 2020-2023 do “Programa das Nações Unidas para os Assentamentos Humanos” (UN-HABITAT, 2019), relativo ao aprimoramento da prosperidade compartilhada em cidades e regiões, foi a necessidade de “implantação ampliada de tecnologias de fronteira e inovações para o desenvolvimento urbano”.

> As tecnologias de fronteira estão influenciando profundamente o surgimento de cidades inteligentes, as formas pelas quais construímos e gerenciamos nossas cidades e outros assentamentos humanos e como os gerentes urbanos tomam decisões mais informadas. Atualmente, incluem, entre outras, a Internet das Coisas, redes de sensores, comunicação máquina a máquina, robótica, inteligência artificial, realidade virtual e aumentada, impressão 3D, sistemas de informação geográfica (SIG), sensoriamento remoto, veículos não tripulados autônomos, drones , blockchain, computação criptográfica e processamento e visualização de big data. A Nova Agenda Urbana pede que as redes de tecnologia e comunicação sejam fortalecidas e que as abordagens de cidades inteligentes usem digitalização, energia limpa e tecnologias para impulsionar o crescimento econômico e melhorar a prestação de serviços, além de promover a inclusão ampla, inclusive de pessoas com deficiência. (UNITED NATIONS, 2019, p. 34, *tradução nossa*)

A ilustração e o quadro que se seguem apresentam casos de uso de tecnologias de IoT para a solução de questões urbanas (BNDES, 2017d). O potencial de impacto dessas soluções justifica a intervenção governamental, para criar um ambiente propício que garanta a implementação das inovações em benefício da sociedade, de forma segura e regulamentada.

Figura 8: Casos de uso de IoT para cidades

Fonte: BNDES (2017c)

Quadro 4: Descrição dos casos de uso de IoT para cidades

Cidades

Cidades (1/2)

Caso de uso	Descrição
• Medidores inteligentes e gestão da demanda de energia	• Redução de custos operacionais de leitura de medidores e prevenção de roubos
• Automação de distribuição e subestações	• Uso de automatização na subestação para reduzir perdas na linha de distribuição, reparo automático dos defeitos na linha, e melhor gerenciamento dos equipamentos da subestação com aparelhos eletrônicos inteligentes
• Medidores de água inteligentes e gestão da demanda	• Redução dos custos operacionais e viabilização da coleta de dados sobre demanda em tempo real – fornecer aos residentes e gerentes de propriedades dados de consumo de água em tempo real para que eles possam identificar onde o consumo está ocorrendo e também onde há vazamentos
• Identificação de vazamentos de água	• Uso de sensores em canos, bombas e demais partes da infraestrutura hidráulica para monitorar as condições e gerenciar perdas por meio de identificação e reparos de vazamentos ou mudança de pressão, conforme a necessidade
• Faixas de congestionamento	• Uso de precificação baseada na demanda para gerenciar o trânsito – tarifas para usar faixas de trânsito ou para dirigir em áreas específicas da cidade
• Precificação e parquímetros inteligentes	• Oferecimento de *insight* em tempo real sobre locais disponíveis, e viabilização da precificação dinâmica para otimizar a oferta e a demanda
• Controle de tráfego centralizado e adaptável	• Uso de câmeras, dados de celulares e sensores para monitorar o tráfego e alterar os semáforos, otimizando o fluxo (p.ex., para ônibus); redirecionamento do tráfego para evitar uma área com problema, e otimizar rotas de ônibus para aumentar a rentabilidade
• Câmeras de trânsito	• Realização de *analytics* em tempo real de *streaming* de vídeos registrados por câmeras que monitoram o trânsito para ajustar os semáforos, otimizando o fluxo
• Coleta inteligente de resíduos sólidos	• Usar *tags* de identificação por radiofrequência para cobrança automática de uma taxa variável de acordo com o uso e otimização das rotas de cobrança com base na necessidade
• Monitoramento da qualidade do ar	• Uso de sensores distribuídos para monitorar partículas suspensas no ar

Cidades

Cidades (2/2)

Caso de uso	Descrição
• Monitoramento da qualidade da água	• Uso de sensores distribuídos para monitorar a qualidade da água nos canos, rios, lagos, etc.
• Atendimento de emergência	• Uso de tecnologias de supervisão, coordenação e transporte para gerenciar e mitigar emergências com mais eficiência
• Monitoramento de crime por vídeo	• Uso de circuito fechado de TV e sistema de monitoramento de áudio para viabilizar resposta e coordenação em tempo real, assim como *analytics* preditiva por meio de dados históricos
• Monitoramento estrutural (iluminação de ruas e pontes)	• Realização de manutenção preventiva sob demanda com sensores localizados na infraestrutura
• Gestão/atualizações de horários de ônibus/trens	• Uso de sensores em ônibus e trens para viabilizar um planejamento melhor das rotas e alavancar o trânsito multimodal
• Monitoramento do transporte público baseado em condições	• Uso de sensores em ônibus e trens para realizar manutenção sob demanda mais eficiente
• Melhoria da eficiência dos equipamentos devido à Internet das Coisas	• Uso de sensores para coleta de dados sobre as condições das rodovias e os padrões de direção – dados usados para aprimorar a eficiência operacional
• Veículos autônomos	• Identificação de usuários próximos de Outdoors de publicidade para oferecimento de anúncios direcionados
• Gestão de desastres	• Uso de sensores distribuídos para detectar ameaças precocemente e coordenar respostas
• Navegação de carros – Cidade	• Carros conectados a outros ativos para aprimorar o monitoramento
• Produtividade humana – Realidade Aumentada	• Realidade aumentada para aplicação da lei, serviços de courier, etc.
• Produtividade humana – Redesenho de RH	• Melhorias organizacionais viabilizadas por dados em tempo real
• Produtividade humana – Monitoramento de atividades	• Gestão de performance de mais qualidade

Fonte: BNDES (2017c)

Um dos principais pontos de necessidade de intervenção governamental é o aspecto regulatório que envolve a IoT. A Agência Nacional de Telecomunicações (Anatel) tem buscado simplificar a regulamentação para remover entraves ao desenvolvimento da tecnologia no país. Em consulta pública, finalizada em outubro

de 2018, foram discutidas questões de outorga, modelo de prestação, roaming internacional, licenciamento, qualidade, numeração, avaliação de conformidade, segurança cibernética, espectro, falhas de infraestrutura e acesso a postes do setor elétrico (GROSSMANN, 2018).

Outro desafio de extrema relevância por parte do governo é a busca pelo alcance do interesse público potencializado pela tecnologia, com foco no bem estar e na qualidade de vida dos cidadãos. Conforme descrito no capítulo 2 e na seção 5.1.1 deste trabalho, há uma forte tendência de que as inovações na área sejam guiadas por motivações primordialmente comerciais ou tecnicistas. Para aproveitar amplamente as possibilidades trazidas pela IoT, o Estado precisa investir em infraestrutura, capacitação e pesquisa, além de garantir inclusão, sustentabilidade, segurança e privacidade nas aplicações.

Considerando a quantidade e disponibilidade de dados coletados, armazenados e processados nas operações de IoT, entram em pauta questionamentos sobre os usos legítimos e as vulnerabilidades das bases de dados. A aplicação de um arcabouço legal consistente, que garanta a privacidade, a proteção de dados pessoais e a segurança jurídica dos cidadãos, com a devida regulação por autoridade competente, tornam-se essenciais nesse contexto.

Como observam Oliveira e Campolargo (2014), as cidades são inteligentes quando “aproveitam ao máximo o capital humano dos seus cidadãos, criam ecossistemas de inovação onde se desenvolvem as novas dinâmicas de criação de riqueza e de emprego e promovem novas formas de governação participativa”. Nesse sentido, a literatura passou a considerar as “*Human Smart Cities*”:

> [...] destacando os diversos projetos de cidades inteligentes que surgiram no mundo e os resultados obtidos até o momento, passou-se a se discutir a necessidade de uma segunda geração de cidades inteligentes, a de cidades humanas inteligentes, a qual busca equilibrar a infraestrutura tecnológica do conceito tradicional com fatores mais soft como: engajamento social, protagonismo cidadão e interação das pessoas em ambientes físicos e virtuais (DEPINÉ et al., 2018, p. 54).

Em 2013, foi criada no âmbito da Frente Nacional de Prefeitos a Rede Brasileira de Cidades Inteligentes e Humanas, entidade sem fins lucrativos, agora representada por um instituto, que reúne integrantes do setor público, de universidades, da sociedade civil e da iniciativa privada para discutir temas e políticas nacionais para o desenvolvimento de cidades inteligentes. De acordo com o conceito adotado pela

Rede, em linhas gerais, é preciso atuar de maneira integrada em cinco camadas para alcançar os objetivos de uma cidade inteligente e humana: pessoas (economia criativa, participação), subsolo (redes de água, esgoto, telefonia, energia, etc.), solo (aspectos urbanos, mobilidade, acessibilidade, sustentabilidade, etc.), infraestrutura tecnológica (parque de iluminação inteligente, rede de fibra ótica, central de operações), e plataforma de internet das coisas (processamento e transparência dos dados gerados e captados) (GOMYDE, 2017).

5.1.4. Políticas relacionadas

Considerando a complexidade e amplitude das políticas voltadas ao ambiente urbano e à regulamentação de tecnologias aplicáveis a esse universo, pretende-se nessa seção apontar as políticas e normativos mais diretamente relacionados aos temas internet das coisas e cidades inteligentes, sem a pretensão de exaustividade.

O Plano Nacional de IoT integra a “Estratégia Brasileira para a Transformação Digital - E-Digital” (BRASIL, 2018), que tem como uma de suas ações estratégicas o fomento de “cidades Inteligentes, utilizando tecnologias provenientes da Internet das Coisas (IoT), como soluções para mobilidade urbana, segurança civil, otimização de *utilities* (energia, água, etc.), com base em ferramentas como *smart grids*, entre outras”.

A iniciativa 064G do PPA 2016-2019 (BRASIL, 2016) - “Lançamento do Plano Nacional de M2M/Internet das Coisas” - vinculava-se de forma direta ao , que apresenta diretrizes para políticas públicas de telecomunicações. Este decreto revogou o “Programa Brasil Inteligente” (Decreto 8.776/2016), bem como os decretos 4.733/2003 (políticas de telecomunicações) e 7.175/2010 (Programa Nacional de Banda Larga - PNBL), ambos relacionados ao tema IoT.

Fazia parte do “Programa Brasil Inteligente” a iniciativa “Minha Cidade Inteligente”, que tinha como objetivo “levar às cidades brasileiras uma rede de fibras ópticas para conectar órgãos públicos e praças de acesso livre a fim de modernizar a gestão municipal e o uso dos serviços do governo”. A iniciativa seria uma evolução do “Programa Cidades Digitais”, que foi objeto de avaliação realizada pelo TCU, Acórdão 1898/2017 (BRASIL, 2017).

Em outubro de 2017, o MCTIC lançou consulta pública para definir o Plano Nacional de Conectividade (PNC), com a premissa substituir o PNBL. A ideia do PNC

seria promover a expansão das redes das operadoras por áreas remotas, universalizando o acesso à internet rápida no Brasil, fator essencial para viabilizar as cidades inteligentes e as soluções de IoT. Após a consulta pública, não foi localizada mais nenhuma notícia sobre o PNC. O Plano dependia de iniciativas do governo, dentre estas, a aprovação da Lei nº 13.879 (BRASIL, 2019c), ocorrida em 03/10/2019, que modifica a Lei Geral de Telecomunicações (BRASIL, 1997). Uma das principais alterações foi a possibilidade de migração do regime de concessão para o de autorização dos serviços de telefonia fixa, com a previsão de aplicação dos saldos da transição em investimentos em banda larga. A lei aguarda ainda regulamentação pela Anatel (AGÊNCIA BRASIL, 2017, 2019).

A imagem a seguir apresenta uma linha do tempo das iniciativas e regulamentos que precederam a atual Estratégia Brasileira para a Transformação Digital - E-Digital (2018a):

Figura 9: Histórico normativo da estratégia brasileira de transformação digital

Fonte: OCDE (2018)

O Plano Nacional de IoT está relacionado também com a iniciativa 04QH do PPA 2016-2019: “Articulação de projetos de pesquisa, desenvolvimento e inovação

em áreas estratégicas de tecnologias digitais com empresas e centros de pesquisa e desenvolvimento (P&D), especialmente na área de segurança cibernética, internet das coisas, big data e computação em nuvem".

Sob a ótica normativa, um marco regulatório fundamental para a implantação de IoT no país foi a publicação da Lei Geral de Proteção de Dados Pessoais – LGPD, Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018a), alterada pela Lei nº 13.853, de 2019. Conforme mencionado em seções anteriores, a coleta e tratamento massivo de dados e a proteção dos dados pessoais são pontos críticos na definição de políticas públicas para IoT. Dada a correlação direta entre a LGPD e o Plano Nacional de IoT, os impactos da norma para as ações do Plano serão detalhados na seção 5.4.1, no âmbito da estratégia de implementação da política. Destaca-se ainda a relevância do Marco Civil da Internet (BRASIL, 2014) nesse cenário.

A Estratégia Nacional de Segurança Cibernética - E-Ciber é mais um dos normativos estritamente relacionados ao Plano Nacional de IoT. Publicada no Decreto nº 10.222, de 2020 (BRASIL, 2020a), a E-Ciber trata das ações governamentais nacionais e internacionais na área, para o quadriênio 2020-2023. Fundamenta-se na Política Nacional de Segurança da Informação, constante do Decreto nº 9.637, de 2018 (BRASIL, 2018b), que "abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade".

No ambiente cidades, destaca-se a relação do Plano do IoT com a Política Nacional de Mobilidade Urbana, lançada em 2012, alterada pela Lei nº 14.000/2020 (BRASIL, 2020d), especialmente no que se refere à criação de plataforma para reunir dados sobre mobilidade nas cidades.

Por fim, a iniciativa governamental mais diretamente vinculada ao escopo deste trabalho é a criação da Câmara para Cidades 4.0 (ou cidades inteligentes), instituída em dezembro de 2019 a partir das prioridades definidas no Plano Nacional de IoT. O colegiado é coordenado pelo MCTIC e pelo Ministério de Desenvolvimento Regional (MDR), com apoio da Anatel e do BNDES. De acordo com o MCTIC (2019), o objetivo da câmara é articular os diversos atores do poder público, do setor privado, da indústria e da academia para o desenvolvimento das cidades inteligentes no Brasil, "além de nivelar as iniciativas em execução nas cidades, estabelecer diretrizes, indicadores padronizados e eixos de atuação para uma Política Nacional para Cidades Inteligentes" (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E

COMUNICAÇÕES, 2019). Nesse sentido, estão em pauta a formulação do “Programa Brasileiro de Cidades Inteligentes Sustentáveis”, com previsão de conclusão até o fim de 2020, e a “Carta Brasileira para Cidades Inteligentes” discutida em audiência pública em fevereiro deste ano (SENADO FEDERAL, 2020).

5.2. Caracterização da política

5.2.1. Objetivos

O Plano Nacional de Internet das Coisas (IoT) foi instituído pelo Decreto nº 9.854, de 25 de junho de 2019 (BRASIL, 2019a), juntamente com a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas (Câmara IoT).

A finalidade da política é “implementar e desenvolver a Internet das Coisas no País com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais”. Pretende-se com o Plano “acelerar a implantação da Internet das Coisas como instrumento de desenvolvimento sustentável da sociedade brasileira, capaz de aumentar a competitividade da economia, fortalecer as cadeias produtivas nacionais e promover a melhoria da qualidade de vida”.

Para fins do normativo (BRASIL, 2019a):

I - “Internet das Coisas – IoT” é definida como “a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade”;

II - “Coisas” são “objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação”;

III - “Dispositivos” são “equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados”; e

IV - "Serviços de valor adicionado" são atividades que acrescentam a um serviço de telecomunicações "novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações" (BRASIL, 1997).

Conforme o Art. 3º do Decreto (BRASIL, 2019a), são objetivos do Plano de IoT:

I - "Melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT";
II - "Promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital";
III - "Incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor";
IV - "Buscar parcerias com os setores público e privado para a implementação da IoT; e
V - "Aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no País". (BRASIL, 2019a).

De acordo com a classificação de Theodore Lowi (1972), o Plano Nacional de IoT pode ser classificado como política pública de cunho distributivo e regulatório. As políticas distributivas geram benefícios concentrados retirando recursos da coletividade sem especificar diretamente sua origem (LOWI, 1972).

> **Políticas distributivas**: são configuradas quando procuram distribuir recursos. Os meios de distribuição podem ser via subsídios em produtos ou serviços, bem como mediante concessão de benefícios diretamente aos interessados. A definição de como os recursos serão distribuídos e de quem serão os beneficiários normalmente é feita por meio de legislação. (PROCOPIUCK, 2013)

Nesse sentido, os recursos destinados ao fomento dos projetos-piloto da política de IoT analisados neste trabalho são distribuídos pelo BNDES, a partir dos critérios apresentados para a seleção das cidades que serão contempladas como público-alvo da implantação das ações, conforme descrito nas seções 5.2.2 e 5.3.1.

As políticas regulatórias, por sua vez, são criadas para estabelecer obrigatoriedades e condições para a realização de determinadas atividades e comportamentos (LOWI, 1972).

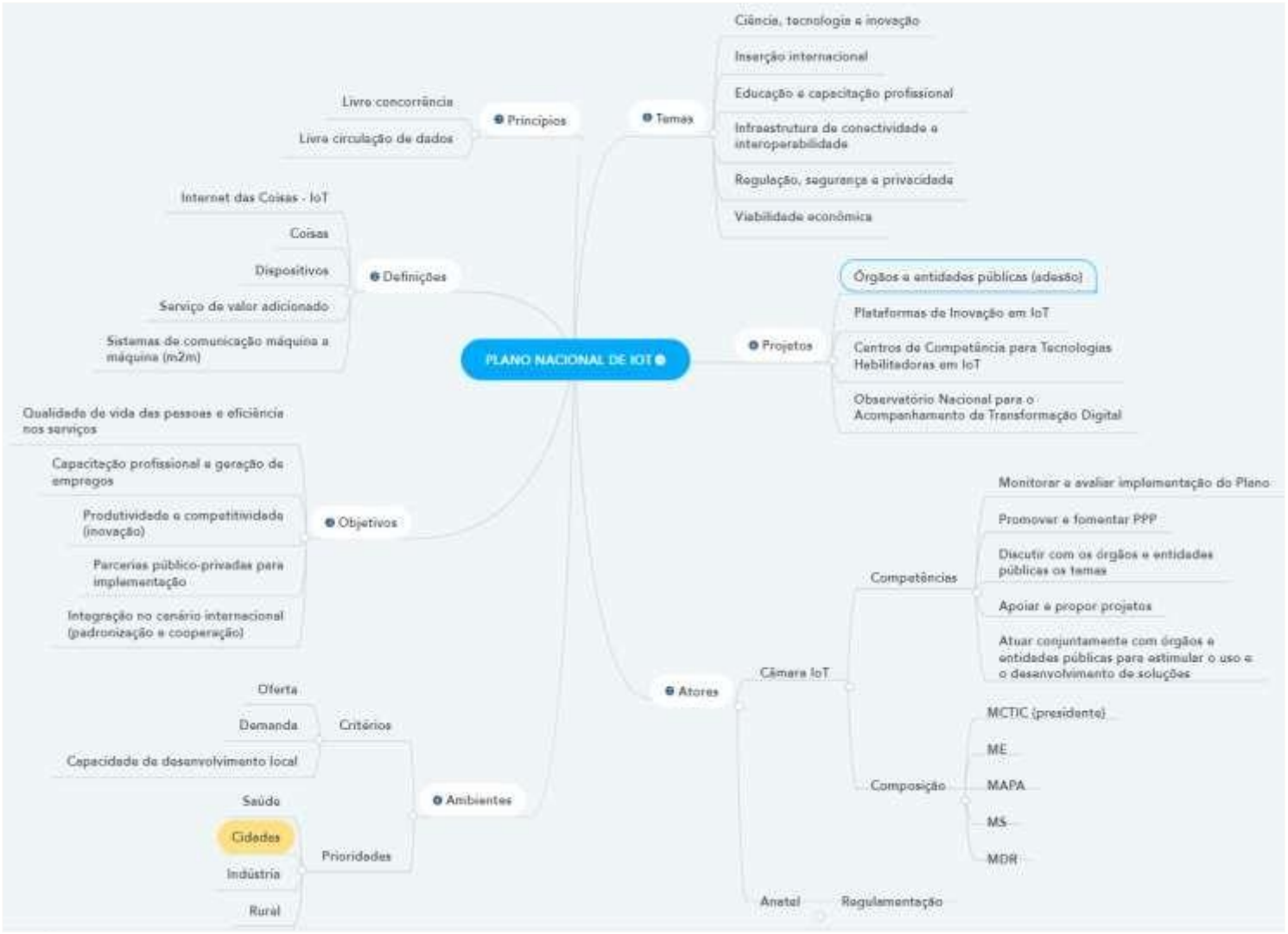
> **Políticas regulatórias:** dizem respeito ao controle estatal sobre a utilização de recursos ou sobre a execução de atividades por diferentes segmentos da sociedade. Normalmente as políticas regulatórias procuram impor padrões de comportamento a indivíduos ou a grupos, com vistas a preservar o interesse público e a manter o equilíbrio em relações competitivas entre os integrantes de dado setor da sociedade.(PROCOPIUCK, 2013).

Do ponto de vista regulatório, o art. 8 do Plano, transcrito a seguir, estabelece a definição das tecnologias abrangidas pela política, cuja especificação traz impactos regulatórios e tributários, discutidos no item 5.4.2.

> Para fins do disposto no art. 38 da Lei nº 12.715, de 17 de setembro de 2012, são considerados sistemas de comunicação máquina a máquina as redes de telecomunicações, incluídos os dispositivos de acesso, para transmitir dados a aplicações remotas com o objetivo de monitorar, de medir e de controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes.
>
> § 1º Para fins do disposto no caput, os sistemas de comunicação máquina a máquina não incluem os equipamentos denominados máquinas de cartão de débito e/ou crédito, formalmente considerados terminais de transferência eletrônica de débito e crédito, classificados na posição 8470.50 da Tabela de Incidência do Imposto sobre Produtos Industrializados - TIPI, aprovada pelo Decreto nº 8.950, de 29 de dezembro de 2016.
>
> § 2º Compete à Agência Nacional de Telecomunicações regulamentar e fiscalizar o disposto neste artigo, observadas as normas do Ministério da Ciência, Tecnologia, Inovações e Comunicações.(BRASIL, 2019a)

O esquema abaixo ilustra os desdobramentos do Plano:

Figura 10: Desdobramentos do Plano Nacional de Internet das Coisas (IoT)



Fonte: elaborado pela autora

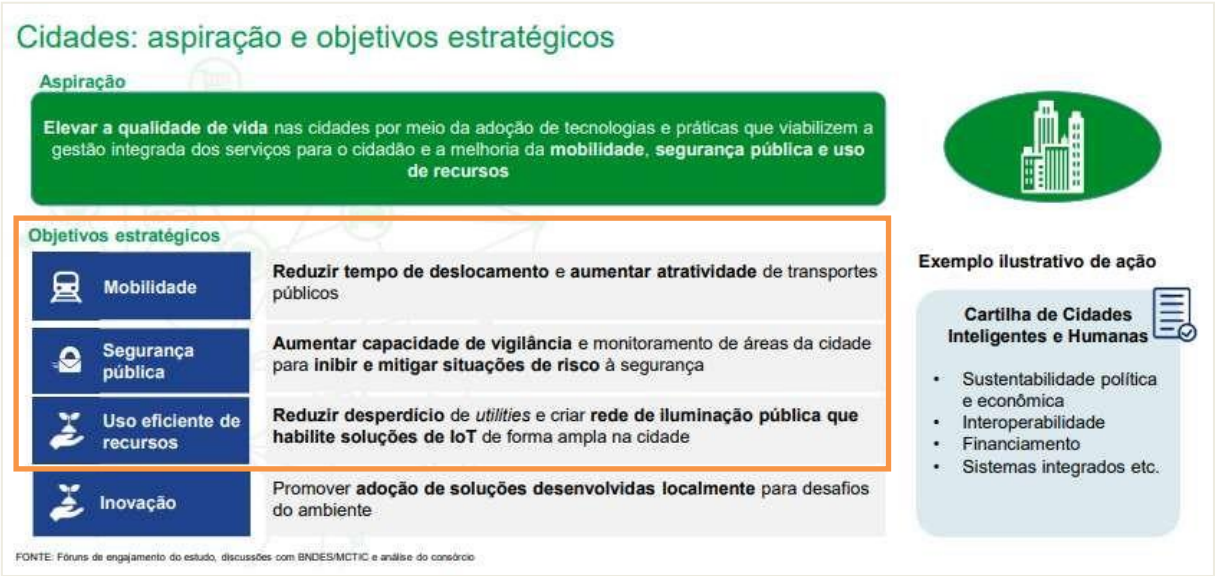
Três pilares definem a estratégia para alcançar a aspiração do país para a IoT (BNDES, 2017d):

Figura 11: Pilares da estratégia brasileira de IoT

Fonte: BNDES (2017d)

Conforme mencionado anteriormente, o foco deste estudo é a vertical “cidades” do Plano de IoT. O quadro abaixo apresenta um resumo da aspiração de IoT para o Brasil e dos objetivos estratégicos para cidades inteligentes, dos quais os três primeiros serão objeto deste trabalho.

Quadro 5: Cidades: aspirações e objetivos estratégicos



Fonte: BNDES (2017d)

5.2.2. Ações e metas

O art. 5º do Decreto nº 9.854 (BRASIL, 2019a) estabeleceu as seguintes temáticas como integrantes do plano de ação com as soluções para viabilizar o Plano Nacional de IoT: I - ciência, tecnologia e inovação; II - inserção internacional; III - educação e capacitação profissional; IV - infraestrutura de conectividade e interoperabilidade; V - regulação, segurança e privacidade; e VI - viabilidade econômica.

O plano de ação foi elaborado a partir dos produtos do estudo do BNDES (2017d), descritos no esquema a seguir. O estudo contou com a participação de atores-chave e especialistas, que elencaram as iniciativas a serem priorizadas até 2022 para a efetiva implantação do ecossistema de IoT no Brasil.

Quadro 6: Fases e produtos do plano de ação de IoT

Fonte: BNDES (2017d)

O plano de ação foi organizado em quatro camadas (ambientes, objetivos estratégicos, objetivos específicos e iniciativas) definidas a partir da aspiração do país para IoT, detalhada no item 5.2.1. A imagem a seguir resume a estrutura do plano, com destaque em laranja para os aspectos tratados neste trabalho:

Quadro 7: Estrutura do plano de ação de IoT

Fonte: BNDES (2017d), destaque da autora

Esta seção trata dos objetivos específicos e das iniciativas do plano de ação (como). Os demais elementos da estrutura do plano já foram abordados nas seções anteriores, com o recorte para o ambiente "cidades inteligentes" e seus objetivos estratégicos (o que). O esquema a seguir resume os quatro objetivos específicos, que refletem as iniciativas, com ênfase em "regulatório, segurança e privacidade", sendo esta última escopo deste trabalho.

Figura 12: Objetivos específicos do plano de ação de IoT

Fonte: BNDES (2017d), destaque da autora

As iniciativas do plano foram categorizadas em ações estruturantes, medidas e elementos catalisadores, conforme descrito no esquema abaixo.

Quadro 8: Categorias de iniciativas do plano de ação para IoT

	Fórum de decisão	Impacto	Facilidade de implantação
Ações estruturantes	▪ Decisões tomadas por alto escalão de órgãos engajados no estudo	▪ Alto e limitado a adoção e desenvolvimento de IoT	▪ Desafiadora porém possível caso haja alinhamento dentro e fora dos órgãos
Medidas	▪ Decisões tomadas por níveis gerenciais de órgãos engajados no estudo	▪ Médio e limitado a adoção e desenvolvimento de IoT	▪ Média e muitas vezes já está em andamento
Elementos catalisadores	▪ Decisões tomadas por fóruns de altíssimo nível, como Presidência da República e Congresso Nacional	▪ Muito alto e não se limita apenas a IoT	▪ Muito desafiadora e, em geral, de resolução de longo prazo

Fonte: BNDES (2017d)

As iniciativas a serem analisadas neste trabalho tratam de privacidade e proteção de dados pessoais, e foram classificadas na horizontal “regulatório” como “elementos catalisadores”, na medida em que seus impactos e implantação ultrapassam as fronteiras do Plano Nacional de IoT. O quadro abaixo lista as duas iniciativas previstas no plano de ação para o tema.

Quadro 9: Elementos catalisadores – privacidade e proteção de dados pessoais

Elementos catalisadores	Privacidade e proteção de dados pessoais	▪ Implantação de **segurança jurídica** para a proteção de dados pessoais. ▪ Definição de autoridade central independente para a **proteção de dados pessoais**, potencialmente em modelo de corregulação.

Fonte: adaptado de BNDES (2017d)

Em relação à criação de autoridade independente para proteção de dados pessoais em modelo de corregulação, o estudo do BNDES sugere que tenha como competências:

> (i) editar normas complementares à legislação federal; (ii) realizar auditoria no tratamento de dados pessoais; (iii) promover ações educacionais; (iv) adotar providências em incidentes de segurança; (v) gerir a transferência de dados pessoais para o exterior; (vi) verificar o cumprimento de normas ou códigos de conduta elaborados em regime de autorregulação; (vii) atuar como ombudsman, recebendo e investigando reclamações individuais contra a má-administração de dados pessoais por entidades públicas e privadas; e (viii) impor sanções diversas (BNDES, 2017b, p. 184).

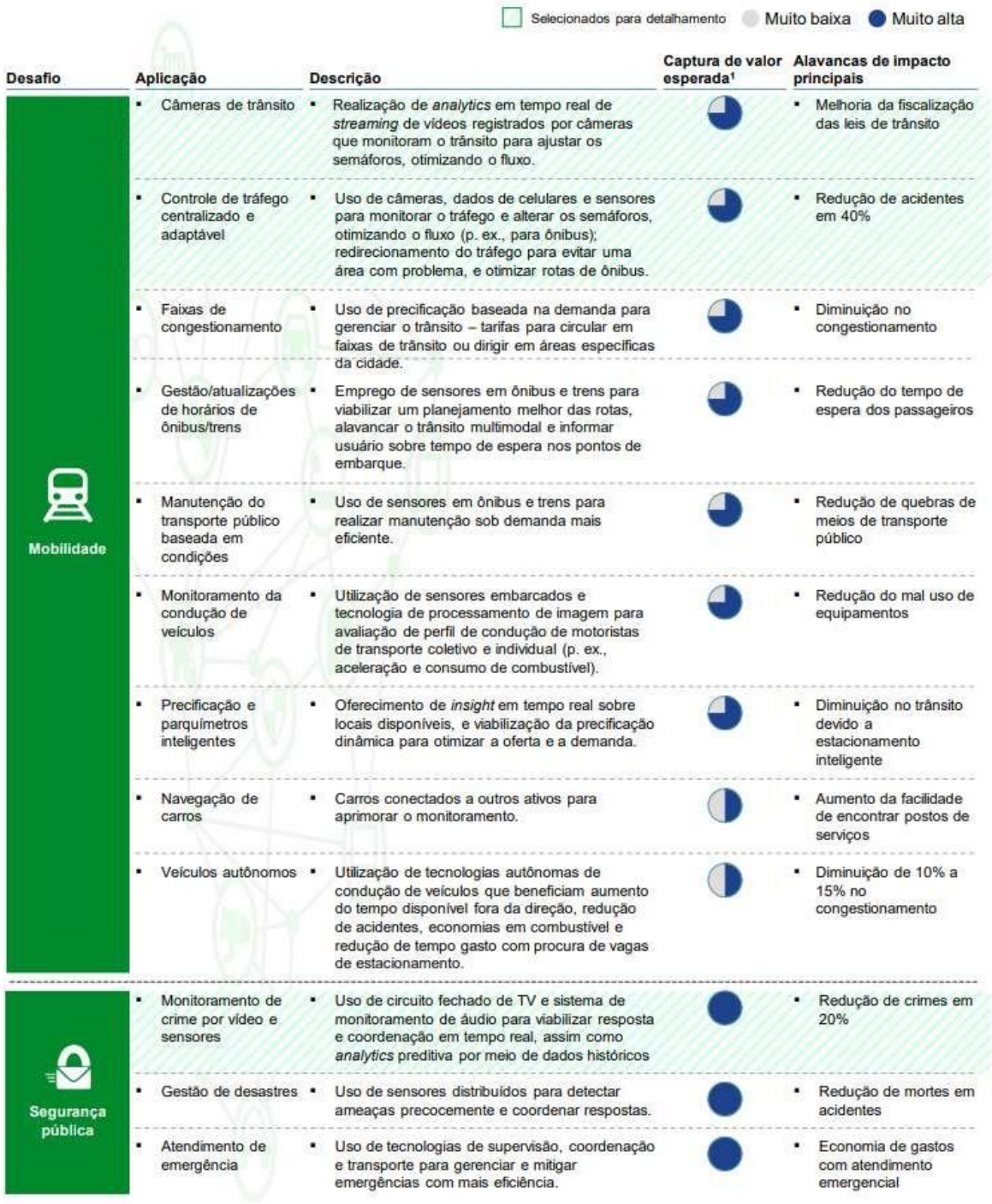
Em termos de implementação da política de IoT no Brasil, as redes de fomento em nível nacional identificadas pelo estudo do BNDES (2017d) como mais diretamente relacionadas ao Plano Nacional de IoT são o próprio BNDES, a Finep – Empresa Brasileira de Inovação e Pesquisa, e a Embrapii - Empresa Brasileira de Pesquisa e Inovação Industrial. Este trabalho concentra-se na análise do programa BNDES Pilotos IoT, que "destina-se a apoiar financeiramente, de forma não reembolsável, projetos inovadores para teste e avaliação de soluções tecnológicas de Internet das Coisas" (BNDES, 2018a).

5.2.3. Resultados e impactos

O estudo do BNDES (2017d) calcula, com base em diversas fontes, que o impacto econômico da IoT no mundo até 2025 será potencialmente de US$ 4 a 11 trilhões. No Brasil, o retorno previsto é da ordem de US$ 50 a 200 bilhões por ano, cerca de 10% do PIB nacional atual. Esse impacto nas cidades em particular deriva de fatores como economias com iluminação pública, monitoramento do tráfego e redução da mortalidade causada pela violência, além da própria movimentação do mercado gerada pelo setor.

O quadro a seguir descreve as potenciais aplicações de IoT para a solução dos problemas elencados na seção 5.1.1, com destaque para os que foram priorizados nos projetos do BNDES Pilotos IoT.

Quadro 10: Principais aplicações e impactos de IoT em cidades



Desafio	Aplicação	Descrição	Captura de valor esperada[1]	Alavancas de impacto principais
Eficiência energética e saneamento	Identificação de vazamentos de água	Uso de sensores em canos, bombas e demais partes da infraestrutura hidráulica para monitorar condições e gerenciar perdas por meio de identificação e reparo de vazamentos ou mudança de pressão, conforme a necessidade.		Redução dos vazamentos de água em 40%-50%
	Medidores inteligentes de energia elétrica	Redução de custos operacionais de leitura de medidores e prevenção de roubos.		Redução de 50% de perdas não técnicas
	Iluminação pública inteligente	Utilização de sensores de monitoramento e de queima de lâmpadas para otimizar o uso e a substituição de ativos de iluminação pública.		Redução de custos operacionais de energia
	Medidores de água inteligentes e gestão da demanda	Redução dos custos operacionais e viabilização da coleta de dados sob demanda em tempo real – fornecer aos residentes e gerentes de propriedades dados de consumo de água em tempo real para que eles possam identificar onde o consumo está ocorrendo e também onde há vazamentos.		Redução da demanda de água em 5%
	Automação de distribuição e subestações de energia	Uso de automatização na subestação para reduzir perdas na linha de distribuição, reparo automático de defeitos na linha, e melhor gerenciamento dos equipamentos da subestação com aparelhos eletrônicos inteligentes.		Redução 4% de perdas nas linhas de transmissão
	Lixeiras inteligentes	Otimização das rotas de coleta de resíduos de lixeiras através do uso de sensores de monitoramento de capacidade.		Redução de custos operacionais na coleta de lixo
	Monitoramento da qualidade da água	Uso de sensores distribuídos para monitorar a qualidade da água nos canos, rios, lagos etc.		Redução de doenças relacionadas à qualidade da agua
	Monitoramento da qualidade do ar	Emprego de sensores distribuídos para monitorar partículas suspensas no ar.		Redução de doenças relacionadas à qualidade do ar
	Tarifação inteligente de resíduos sólidos	Uso de *tags* de identificação por radiofrequência para cobrança automática de taxa variável de acordo com o consumo.		Melhoria da produtividade em 23%
Outros	Monitoramento estrutural (iluminação de ruas e pontes)	Realização de manutenção preventiva sob demanda com sensores localizados na infraestrutura.		Economia com gastos na manutenção de iluminação e pontes
	Anúncios geolocalizados no transporte publico	Seleção de anúncios em tempo real de acordo com região de passagem do transporte público.		Melhoria na taxa de retorno dos investimentos em publicidade
	Melhoria da eficiência de ativos por meio de IoT	Uso de sensores para coleta de dados sobre as condições das rodovias e os padrões de direção, por exemplo, usando dados para aprimorar a eficiência operacional.		Economia de custo operacional de manutenção de ativos
	Realidade aumentada para crescimento de produtividade humana	Uso de realidade aumentada para aplicação da lei e de serviços de correio, por exemplo.		Economia no uso de mão de obra e aumento da agilidade

1 Estimativa qualitativa realizada junto à equipe de especialistas setoriais do BNDES

Fonte: BNDES (2017d)

O BNDES Pilotos IoT declarou como diretrizes, resumidamente: (i) induzir a cooperação em soluções de IoT nos três ambientes (cidades, rural e saúde); (ii) incentivar a adoção de IoT por meio de financiamento; (iii) assegurar a continuidade dos esforços desenvolvidos e articular parcerias nas áreas selecionadas; e (iv) fomentar a aproximação entre ITs, empresas e outros parceiros, incluindo startups e demandantes potenciais das soluções de IoT (BNDES, 2018a).

Como impactos esperados, foram elencados: (i) identificar oportunidades de otimizações das soluções implementadas; (ii) avaliar a aceitação dos usuários e estimular a discussão de temas críticos ao uso de IoT, incluindo privacidade e segurança; (iii) promover o desenvolvimento e difusão da IoT nos ambientes priorizados em aplicações reais, apoiando a construção de modelos de negócio em larga escala; (iv) reduzir a assimetria de informação entre usuários e fornecedores; (v) induzir investimentos em IoT, tanto em soluções quanto em infraestrutura e PD&I, contribuindo para o desenvolvimento setorial; (vi) promover ambiente de inovação e empreendedorismo; e (vii) estimular a cooperação continuada entre os atores envolvidos (BNDES, 2018a).

5.3. Desenho e implementação da política

5.3.1. Público-alvo, priorização e vigência

O Decreto nº 9.854/2019 (BRASIL, 2019a), que materializou o Plano Nacional de IoT, conferiu ao MCTIC a atribuição de priorizar os ambientes para aplicações de soluções de IoT. A indicação é utilizada como base para “o acesso a mecanismos de fomento à pesquisa científica, ao desenvolvimento tecnológico e à inovação”; e para “o apoio ao empreendedorismo de base tecnológica”. A seleção ocorreu a partir de critérios de oferta, demanda e capacidade de desenvolvimento local.

Foram priorizados os ambientes cidades, saúde e rural, detalhados abaixo. Destaca-se para análise o ambiente cidades, com os objetivos das respectivas áreas de atuação (mobilidade, segurança pública, eficiência energética e saneamento).

Quadro 11: Ambientes priorizados

Fonte: (BNDES, 2018a)

Em 2018, o BNDES lançou o processo seletivo “Pilotos IoT” (2018a) com o intuito de contemplar projetos-piloto de soluções inovadoras de IoT para apoio financeiro nos três ambientes priorizados. Ao todo, foram disponibilizados R$ 30 milhões em recursos não reembolsáveis: A participação do banco é de até 50% dos itens financiáveis, com valor mínimo de R$ 1 milhão para cada projeto, sendo o valor global financiável de pelo menos R$ 2 milhões, com prazo de execução de até 24 meses.

O projeto-piloto abrange os casos de usos que serão testados em plataformas de experimentação ou em ambientes reais, como as cidades. A execução deve considerar a integração de tecnologias e arquiteturas de IoT (dispositivos, rede, suporte a aplicações e segurança), priorizando a replicação em larga escala; a avaliação técnica e econômica de impacto, incluindo a viabilidade do modelo de

negócio; e questões de segurança, privacidade e confiabilidade. Estão no escopo do financiamento (BNDES, 2018a):

- Instituições tecnológicas (IT)**,** públicas ou privadas, sem fins lucrativos, que tenham por missão a pesquisa básica ou aplicada de caráter científico ou tecnológico, bem como desenvolvimento; e
- Instituições de apoio (IA) a projetos de pesquisa, ensino e extensão e de desenvolvimento institucional, científico e tecnológico de interesse de instituições federais, estaduais ou municipais de ensino superior ou de instituições de pesquisa científica e tecnológica.

Figura 13: BNDES Pilotos IoT – processo de priorização

Fonte: BNDES (2018a)

O BNDES concluiu a etapa de enquadramento dos projetos, que foram selecionados por grupos multidisciplinares de avaliação, um para cada ambiente, formados por integrantes internos e externos ao banco. Os planos foram aprovados pelo Comitê de Elegibilidade de Operações e Crédito (CEC), composto pelos superintendentes do banco. Para o ambiente cidades, foram contempladas as seguintes instituições, com as respectivas propostas e cidades para teste:

- Centro de Pesquisas e Desenvolvimento em Telecomunicações (CPqD): i) uso de câmeras e visão computacional para segurança pública; ii) predição avançada do clima; iii) provimento do serviço de veículos elétricos

compartilhados; iv) plataforma completa de telegestão para iluminação pública. Município: Campinas/SP.

- Fundação Instituto Nacional de Telecomunicações (Finatel): implantação de telegestão na rede de iluminação inteligente e integração com videomonitoramento para segurança pública. Municípios: Santa Rita do Sapucaí/MG, Caxambu/MG e Piraí/RJ.
- Fundação para Inovações Tecnológicas (Fitec): implantação de rede de iluminação pública habilitadora de soluções de IoT, tais como lixeiras inteligentes, videomonitoramento para segurança pública, defesa civil e parquímetros eletrônicos. Município: Mar de Espanha/MG
- Instituto Atlântico: implantação de redes de iluminação pública habilitadoras de soluções de IoT, visando a redução do tempo de deslocamento, aumento da atratividade de transportes públicos e o aumento da capacidade de vigilância para segurança pública. Municípios: Fortaleza/CE, Juazeiro do Norte/CE e Petrópolis/RJ.
- Laboratório de Sistemas Integráveis Tecnológico (LSI-TEC): utilização de Single Board Computer “Labrador” para i) controle inteligente da rede semafórica da cidade de São Paulo e ii) monitoramento de situações de crime e ameaças à segurança urbana. Município: São Paulo/SP.

A figura abaixo ilustra exemplos de aplicações selecionadas em cidades:

Figura 14: Aplicações selecionadas para cidades inteligentes

Fonte: BNDES (2018a)

Os demais investimentos governamentais ou oriundos de parcerias público-privadas em IoT identificados não estão no escopo deste trabalho. A título de ilustração, das iniciativas decorrentes do Plano Nacional de IoT e do potencial do setor, destacam-se:

- FIP-IoT - Fundo de Investimento em Participações em Internet das Coisas – lançou em dezembro de 2019 edital de chamada pública para seleção na categoria Capital Semente, pela BNDESPAR, em parceria com a Qualcomm Ventures, em consonância com a ICVM 578/2016 (COMISSÃO DE VALORES MOBILIÁRIOS, 2016). Além do Plano Nacional de IoT, a chamada tem como fundamento a Portaria MCTIC nº 5.894 (BRASIL, 2018b), que regulamenta o uso de recursos da Lei de Informática em Fundos de Venture Capital. O prazo de duração do fundo é de 10 (dez) anos, prorrogáveis por mais 02 (dois) e o período de investimento são os 05 (cinco) primeiros anos. Como portfólio-alvo, o capital é destinado a empresas de base tecnológica sediadas no Brasil, em quaisquer verticais de mercado, com faturamento bruto de até R$ 16 (dezesseis) milhões/ano. É desejável que o fundo invista em pelo menos 14 (quatorze) empresas, em todo o território nacional. As demais informações sobre a seleção podem ser consultadas no edital (BNDES, 2019).

- Finep IoT - financiamento reembolsável, operado pela Finep, com recursos do FNDCT (Fundo Nacional de Desenvolvimento Científico e Tecnológico), tem por objetivo o "desenvolvimento de novos produtos, processos e serviços baseados em tecnologias digitais" como IoT com aplicações em saúde, indústria, agronegócio e desenvolvimento urbano. O público alvo são empresas brasileiras com receita igual ou superior a R$ 16 milhões, com propostas de no mínimo R$ 5 milhões (FINEP, 2018).
- PPI IoT/Manufatura 4.0 - Programa de Parcerias de Investimentos (PPI) em IoT/Manufatura 4.0, do MCTIC, coordenado pela Embrapii, com recursos captados de empresas beneficiadas pela Lei de Informática. Tem como foco investimentos em pesquisa, desenvolvimento e inovação (PD&I), e pode contemplar de startups a empresas consolidadas no mercado. Projetos em conjunto podem garantir até 50% de recursos não reembolsáveis (EMBRAPII, 2019).

5.3.2. Agentes envolvidos, gestão e governança

Os agentes diretamente envolvidos com o Plano Nacional de IoT são: o MCTIC, órgão responsável pela implementação, o Ministério da Economia e o BNDES. Compõem o ecossistema da IoT agentes governamentais e econômicos, além de instituições científicas, tecnológicas e de inovação, articulados com a iniciativa privada e a sociedade civil, com a finalidade de prospectar oportunidades de desenvolvimento na área.

O MCTIC instalou, em 2014, a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas (Câmara IoT), fórum multisetorial (Decreto 8.234/2014) que vem articulando a construção da política pública para a IoT no país (BRASIL, 2018a). O Decreto nº 9.854 (BRASIL, 2019a) recriou o órgão com composição interministerial. Presidida pelo MCTIC, a Câmara IoT conta atualmente com a participação de 65 instituições, listadas no Anexo 1, incluindo órgãos de governo, iniciativa privada, universidades e centros de pesquisa.

A Câmara IoT é, portanto, órgão de assessoramento destinado a acompanhar a implementação do Plano Nacional do IoT, a quem compete: I - monitorar e avaliar as iniciativas de implementação do Plano; II - promover e fomentar parcerias entre

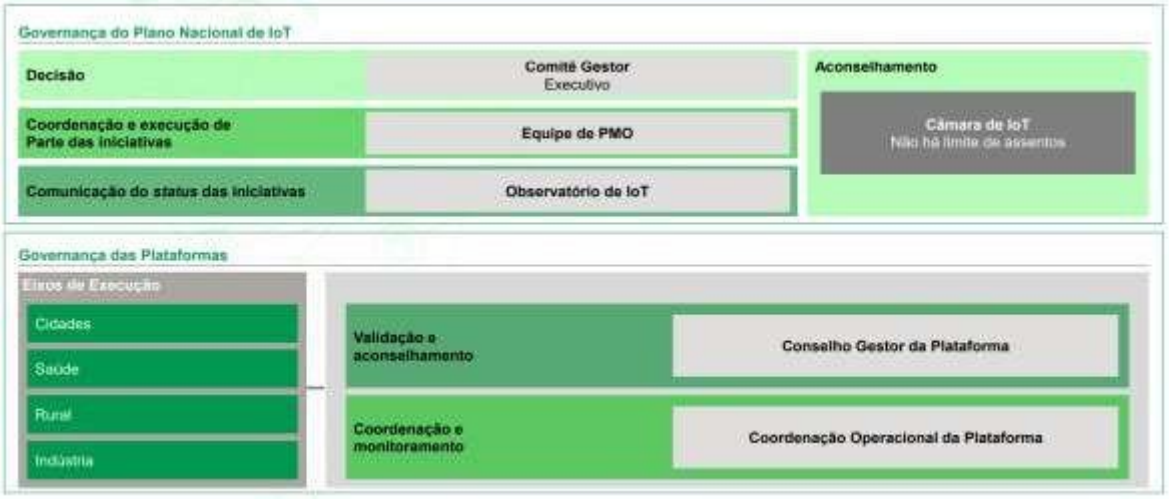
entidades públicas e privadas para o alcance dos objetivos do Plano Nacional de IoT; III - discutir com os órgãos e entidades públicas os temas do plano de ação; IV - apoiar e propor projetos mobilizadores; e V - atuar conjuntamente com órgãos e entidades públicas para estimular o uso e o desenvolvimento de soluções de IoT (BRASIL, 2019a).

Além da Câmara IoT, foi lançado em 2012 o Fórum de IoT, para promover a integração, troca de experiências e criação de uma agenda estratégica na área. Outras instituições que compõem a estrutura de governança da IoT são: Grupo de Trabalho sobre Manufatura Avançada, Frente Parlamentar Mista em Apoio às Cidades Inteligentes, Associação Brasileira de Internet Industrial e Associação Brasileira de Internet das Coisas.

Dentre as agências reguladoras dos setores especificamente afetados pela política de IoT, destaca-se o papel da Anatel como ator fundamental, a quem cabe regulamentar e fiscalizar o disposto no Plano Nacional de IoT, em consonância com as normas do MCTIC; e o da Agência Nacional de Energia Elétrica – Aneel, no que diz respeito às questões específicas do eixo “eficiência energética” das cidades inteligentes. Ressalta-se ainda o papel fundamental da recém criada mas ainda não implantada “Autoridade Nacional de Proteção de Dados”, integrante da Presidência da República, estabelecida na LGPD como “órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (BRASIL, 2018a, 2019b).

O estudo do BNDES propõe o modelo de governança a seguir para a política de IoT. Como crítica, indica a necessidade de maior articulação com o ecossistema internacional do setor (BNDES, 2017d).

Quadro 12: Governança do Plano Nacional de IoT



Fonte: BNDES (2017d)

Os seguintes projetos mobilizadores foram instituídos como elementos de governança pelo Plano Nacional de IoT, coordenados pelo MCTIC (BRASIL, 2018b):

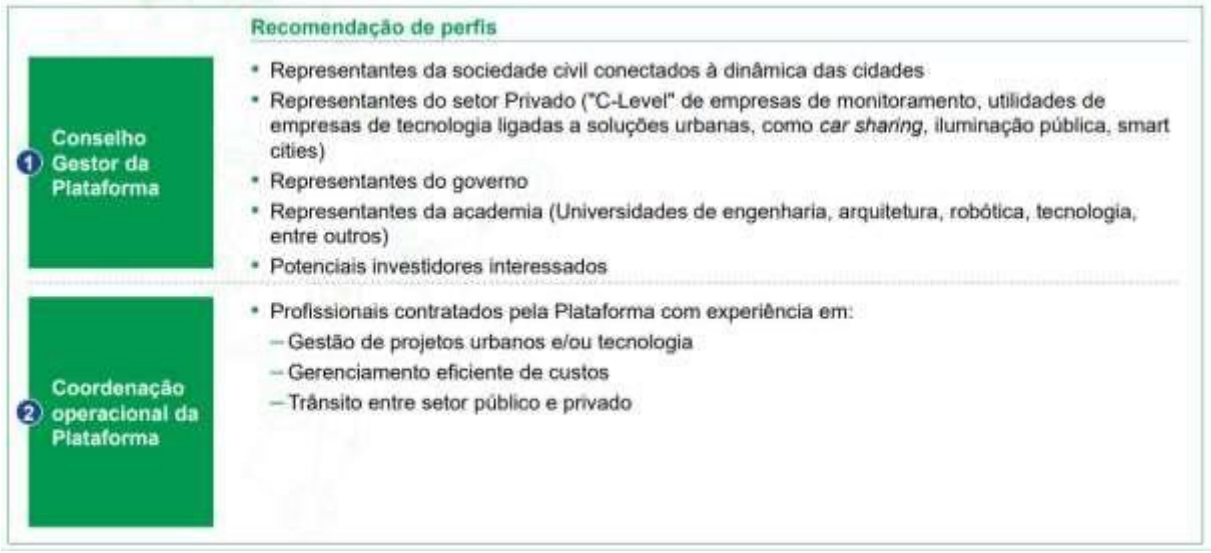
(I) Plataformas de Inovação em Internet das Coisas;

(II) Centros de Competência para Tecnologias Habilitadoras em Internet das Coisas; e

(III) Observatório Nacional para o Acompanhamento da Transformação Digital.

Especificamente para a Plataforma Cidades (item I), foi sugerida pelo estudo do BNDES (2017d) a seguinte estrutura:

Quadro 13: Governança da Plataforma Cidades



Fonte: BNDES (2017d)

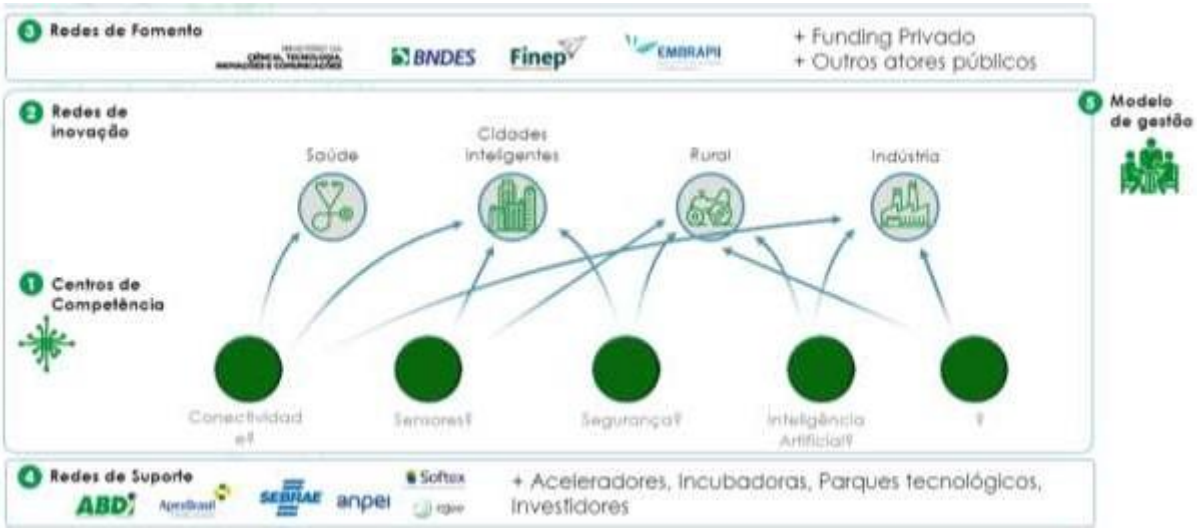
O estudo propõe ainda um guia para a aplicação de IoT em cidades, que tem como base a Cartilha de Cidades, publicada pelo BNDES (2018b), e o apoio no planejamento e na execução dos projetos-piloto nas áreas priorizadas. As ações são direcionadas ao apoio técnico, financiamento e capacitação, para promover a adoção soluções de IoT por centros urbanos brasileiros.

Quadro 14: Proposta de apoio para IoT em Cidades

Fonte: BNDES (2017d)

O esquema a seguir apresenta de forma simplificada um modelo de coordenação entre os principais atores envolvidos com o ecossistema de inovação da IoT (item II). Na seção 5.5 são descritos os aportes financeiros da Redes de Fomento.

Figura 15: Ecossistema de inovação - IoT



Fonte: BNDES (2017d)

O Observatório Nacional para o Acompanhamento da Transformação Digital (item III) foi lançado pelo MCTIC como um portal de acompanhamento das ações sobre o tema, em parceria com o Movimento Brasil Competitivo e o CPqD. A ideia é criar sinergia entre os diversos atores, como governo, empresas, centros de pesquisa, startups, sociedade civil. O portal publica indicadores e fontes de financiamento, bem como as principais ações do governo federal para o alcance dos objetivos estabelecidos e para o monitoramento de políticas públicas na área, dentre as quais a E-Digital e o Plano Nacional de IoT (OBSERVATÓRIO DA TRANSFORMAÇÃO DIGITAL, 2018b).

Conforme diagnóstico das horizontais do relatório do BNDES:

> Para que o ecossistema de IoT avance são necessários mecanismos de governança sólidos para fortalecer a cooperação entre o governo, centros de pesquisa e universidades, empresas e a sociedade. O objetivo desses mecanismos é impulsionar o ecossistema de inovação e desenvolvimento de soluções em IoT, organizando demandas difusas no setor. Um bom sistema de governança concentra e canaliza esforços para atacar os principais gargalos. Os mecanismos podem variar desde associações ativas na promoção das pautas relevantes para essa tecnologia até consórcios e competições promovidas por órgãos governamentais (BNDES, 2017d, p. 32).

A IoT deve ser uma plataforma de rede orientada às pessoas, na qual as comunidades criem valor a partir de múltiplas contribuições individuais, de modo que o ambiente futuro é aquele que vai depender não apenas de grandes centros de supercomputação e do governo, mas das práticas de várias matrizes de indivíduos em constante mudança, voltados à concepção de novos ambientes (YAN et al., 2008).

5.3.3. Modelo lógico

Optou-se por adotar a ferramenta de Modelo Lógico para representar de forma sequencial e sistemática os insumos, atividades, produtos, resultados e impactos da política analisada, conforme indicação do Guia Prático de Análise *Ex Ante* (2018), no intuito de “exibir a racionalidade que sustenta [a] política, identificar e descrever os diversos componentes do desenho, das operações e dos efeitos esperados”. Os valores apresentados nos insumos são os que foram executados pelo BNDES para a realização dos projetos-piloto do plano. Os demais valores previstos estão descritos no item 5.5.

Quadro 15: Modelo Lógico do Plano Nacional de IoT - Cidades Inteligentes

EIXO	PROBLEMA	BENEFICIÁRIOS	EXECUTORA	INSUMOS*	ATIVIDADES	PRODUTOS	RESULTADOS | IMPACTOS
BNDES Estudo "Internet das Coisas: um plano de ação para o Brasil" 2018-2022							
IoT Geral	Necessidade de diagnóstico e proposição de políticas públicas no tema Internet das Coisas no Brasil.	Brasil	McKinsey	R$ 6.726.987,00	Diagnóstico; seleção de verticais e horizontais; elaboração de plano de ação.	Estudo "Internet das Coisas: um plano de ação para o Brasil" 2018-2022 - 14 relatórios de estudo e 5 workshops.	Obter visão geral do impacto de IoT no Brasil e definir aspirações do país; definir critérios para seleção e priorização de projetos; entender competências de TIC no país.
			CPqD	R$ 825.000,00			
			Pereira Neto/ Macedo	R$ 2.246.720,00			
			TOTAL	**R$ 9.798.707,00**			
Pilotos IoT - Cidades Inteligentes							
Segurança pública	**Incidentes:** o Brasil está entre os 20 paises mais violentos do mundo (UNODC, 2019).	Campinas (SP)	**CPqD** - Centro de Pesquisas e Desenvolvimento em Telecomunicações	R$ 2.975.326,00	Implantação de câmeras e visão computacional para segurança pública.	Serviço de videomonitoramento, com câmeras de alta definição, auxiliado por visão computacional, para segurança pública e identificação de veículos.	Aumentar a capacidade de vigilância e monitoramento das áreas da cidade para mitigar situações de risco à segurança
Eficiência energética e saneamento	**Gestão e distribuição de recursos básicos:** iluminação pública consome cerca de 4% da energia elétrica do páis, com potencial de ganho de eficiência de 40%.				Medição de microclima na área urbana.	Estações meteorológicas compactas e conectadas, integradas a sensores de nível de rios em pontos estratégicos da cidade.	Fornecer dados relevantes, no tempo apropriado, para a Defesa Civil emitir alertas que poderão mitigar o impacto causado por desastres ambientais.
					Implantação de plataforma completa de telegestão para iluminação publica.	Serviço de microlocalização de ativos e conectividade das estações meteorológicas compactas.	Melhorar a prestação do serviço de iluminação pública, principalmente tarifação baseada no consumo real de energia, além de habilitar novos modelos de negócios para serviços que agreguem valor à rede de iluminação pública.
Mobilidade	**Transporte público:** 3 das 5 cidades mais congestionadas do mundo são brasileiras.				Provimento do serviço de veículos elétricos compartilhados.	Veículos elétricos compartilhados.	Aprimorar a segurança e a mobilidade urbana.
Eficiência energética e saneamento	**Gestão e distribuição de recursos básicos:** iluminação pública consome cerca de 4% da energia elétrica do páis, com potencial de ganho de eficiência de 40%.	Santa Rita do Sapucaí (MG), Caxambu (MG) e Piraí (RJ)	**Finantel** - Fundação Instituto Nacional de Telecomunicações	R$ 1.438.421,00	Implantação de telegestão na rede de iluminação inteligente.	Rede de iluminação inteligente.	Criar rede de iluminação pública que habilite soluções de IoT de forma ampla na cidade.
Segurança pública	**Incidentes:** o Brasil está entre os 20 paises mais violentos do mundo (UNODC, 2019).				Integração com videomonitoramento para segurança pública.	Videomonitoramento.	Aumentar a capacidade de vigilância e monitoramento das áreas da cidade para mitigar situações de risco à segurança.

EIXO	PROBLEMA	BENEFICIÁRIOS	EXECUTORA	INSUMOS	ATIVIDADES	PRODUTOS	RESULTADOS | IMPACTOS
Pilotos IoT - Cidades Inteligentes							
Eficiência energética e saneamento	**Gestão e distribuição de recursos básicos:** iluminação pública consome cerca de 4% da energia elétrica do país, com potencial de ganho de eficiência de 40%.	Mar de Espanha (MG)	**Fitec -** Fundação para Inovações Tecnológicas		Implantação de rede de iluminação pública habilitadora de soluções de IoT, tais como lixeiras inteligentes.	Rede de iluminação pública habilitadora de soluções de IoT, tais como lixeiras inteligentes.	Reduzir desperdício de utilities e criar rede de iluminação pública que habilite soluções de IoT de forma ampla na cidade.
Segurança pública	**Incidentes:** o Brasil está entre os 20 países mais violentos do mundo (UNODC, 2019).				Implantação de rede com videomonitoramento para segurança pública, defesa civil e parquímetros eletrônicos.	Videomonitoramento para segurança pública, defesa civil e parquímetros eletrônicos.	Aumentar a capacidade de vigilância e monitoramento das áreas da cidade para mitigar situações de risco à segurança.
Eficiência energética e saneamento	**Gestão e distribuição de recursos básicos:** iluminação pública consome cerca de 4% da energia elétrica do país, com potencial de ganho de eficiência de 40%.	Fortaleza (CE), Juazeiro do Norte (CE) e Petrópolis (RJ)	**Instituto Atlântico**	Não disponível (BNDES)	Implantação de redes de iluminação pública habilitadoras de soluções de IoT.	Redes de iluminação pública habilitadoras de soluções de IoT para mobilidade urbana e segurança pública.	Criar rede de iluminação pública que habilite soluções de IoT de forma ampla na cidade.
Mobilidade	**Transporte público:** 3 das 5 cidades mais congestionadas do mundo são brasileiras.						Reduzir tempo de deslocamento e aumentar atratividade de transportes públicos.
Segurança pública	**Incidentes:** o Brasil está entre os 20 países mais violentos do mundo (UNODC, 2019).						Aumentar capacidade de vigilância para segurança pública.
Mobilidade	**Transporte público:** 3 das 5 cidades mais congestionadas do mundo são brasileiras.	São Paulo (SP)	**LSI-TEC -** Laboratório de Sistemas Integráveis Tecnológico	R$ 2.626.790,00	Controle inteligente da rede semafórica.	Serviço de Single Board Computer "Labrador".	Reduzir tempo de deslocamento e aumentar atratividade de transportes públicos.
Segurança pública	**Incidentes:** o Brasil está entre os 20 países mais violentos do mundo (UNODC, 2019).				Monitoramento de situações de crime e ameaças à segurança urbana.		Aumentar capacidade de vigilância para segurança pública.
			TOTAL	**R$ 7.040.537,00**			
BNDES			**INVESTIMENTO TOTAL:**	**R$ 16.839.244,00**			

* Recursos financeiros do BNDES, não reembolsáveis (até 50% do valor total dos itens financiáveis).

Fonte: elaborado pela autora, com dados do BNDES (2018a, 2020) e CPqD (2019)

5.4. Normativos e regulação

Essa seção analisa questões normativas e regulatórias relacionadas à implementação do Plano Nacional de IoT, particularmente no que tange à intersecção entre as áreas priorizadas da vertical cidades inteligentes e os aspectos da horizontal regulatória relativos à privacidade.

5.4.1. Instrumentos normativos

Privacidade em cidades inteligentes

O diferencial de uma “cidade inteligente” é sua capacidade de gerenciar a camada exponencial de dados extraídos das interações entre pessoas e dispositivos de forma integrada, em prol da eficiência urbana e da qualidade de vida dos cidadãos. Com a instrumentação dos serviços com sensores, atuadores e sistemas baseados em inteligência artificial, capazes de processar grandes quantidades de dados, torna-se possível realizar uma gestão pública mais moderna e eficiente, com tomada de decisões fundamentadas em evidências para políticas públicas. Dados são, portanto, ponto crítico das soluções de IoT para cidades.

Políticas de cidades inteligentes devem ter como princípio o foco nas pessoas, buscando a melhoria da experiência dos cidadãos. A gestão de políticas públicas baseada em dados, a busca pela transparência das ações governamentais e a garantia de direitos fundamentais como privacidade e proteção de dados pessoais são pilares de uma estratégia de “governo inteligente”, que busca aprimorar o relacionamento entre cidadão, governo e iniciativa privada.

A regulamentação do uso de dados a serviço do interesse público deve ser pautada em princípios como legalidade, transparência, finalidade e consentimento. O desafio é buscar o equilíbrio entre as prerrogativas do Estado, como garantia da segurança pública, e as liberdades dos cidadãos. Além do arcabouço legislativo, municípios e estados devem definir e tornar públicas boas práticas que garantam em âmbito local esses direitos (BNDES, 2018b).

A responsabilidade por assegurar a privacidade dos cidadãos é das três esferas de governo. É preciso garantir a disponibilidade e a transparência dos dados, em consonância com os princípios de impessoalidade, publicidade e eficiência. Transparência refere-se tanto à prestação de informações solicitadas quanto à declaração de políticas de privacidade, que devem informar aos cidadãos sobre os métodos de coleta, armazenamento, processamento, compartilhamento e acesso aos dados pessoais. A disponibilidade torna-se mais efetiva pela adoção de padrões de dados abertos e interoperáveis (BNDES, 2018b).

As soluções de IoT implementadas pela iniciativa privada ou pelo governo que utilizem dados para finalidades que extrapolam a prestação de serviço público requerem consentimento válido dos titulares. Uma boa prática é a implementação de

funcionalidade de *opt-in,* pela qual o usuário concorda com os termos propostos para a coleta de dados; e *opt-out,* para cessar a qualquer momento a coleta ou tratamento de dados pessoais. Outra é evitar coletar dados pessoais considerados sensíveis (BNDES, 2017b).

Destacam-se como instrumentos normativos com impactos substanciais para as aplicações de IoT em termos de privacidade em cidades inteligentes a Lei Geral de Proteção de Dados Pessoais – LGPD (BRASIL, 2018a) e o Marco Civil da Internet (BRASIL, 2014). Outras normas que merecem destaque, sem a pretensão de contemplar exaustivamente o quadro legal afeto ao tema, são a Estratégia de Governo Digital (BRASIL, 2020b), a Política Nacional de Segurança da Informação – PNSI (BRASIL, 2018b), e o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados (BRASIL, 2019d).

No quadro abaixo foram elencados os pontos das normas mais diretamente relacionados às questões em pauta neste trabalho (privacidade e proteção de dados):

Quadro 16: Instrumentos normativos aplicáveis à IoT

Lei nº 13.709/2018	Lei Geral de Proteção de Dados - LGPD
Ementa	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.
Fundamentos	Respeito à privacidade; autodeterminação informativa; inviolabilidade da intimidade, da honra e da imagem; desenvolvimento econômico e tecnológico e a inovação; livre iniciativa, a livre concorrência e a defesa do consumidor; e direitos humanos, livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
Princípios	Finalidade: tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível; Adequação: compatibilidade do tratamento com as finalidades informadas ao titular; Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos; Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; 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; Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; 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; Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; 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.
Escopo	Qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que realizada no território nacional.
	Não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais.

Lei nº 13.709/2018	**Lei Geral de Proteção de Dados - LGPD**
Disposições	**Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável; **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; 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); 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; Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
	Tratamento de dados pessoais: Mediante o fornecimento de consentimento pelo titular; para o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições desta Lei; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiro.
	Tratamento de dados pessoais sensíveis: Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; Sem fornecimento de consentimento do titular, se indispensável para: cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; proteção da vida ou da incolumidade física do titular ou de terceiro; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados nesta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Lei nº 13.709/2018	Lei Geral de Proteção de Dados - LGPD
Disposições	Dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
	Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. 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.
	O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.
	As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, exceto quando estiverem operacionalizando políticas públicas, em que terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.
	Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas.
	A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular.
	Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança [dos dados].
Legislação relacionada	Alterada pela Lei nº 14.010/2020, que mantém o início da vigência da LGPD para **3/5/2021** e prorroga o prazo para início das sações administrativas para **1/8/2021.**
	Alterada pela Lei nº 13.853/2019 - para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados.
Alterações	Em nenhum caso a totalidade dos dados pessoais de banco de dados poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. O tratamento posterior dos dados pessoais 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. O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, integrada pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. É assegurada autonomia técnica e decisória à ANPD.

Lei nº 12.965/2014	Marco Civil da Internet
Ementa	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Fundamentos	Direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; pluralidade e a diversidade; abertura e colaboração; livre iniciativa, a livre concorrência e a defesa do consumidor; e finalidade social da rede.
Princípios	Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; proteção dos dados pessoais, na forma da lei; responsabilização dos agentes de acordo com suas atividades;, nos termos da lei; liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios.
Disposições	O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; inviolabilidade e sigilo do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas, salvo por ordem judicial;; informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet; 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; informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta; não sejam vedadas pela legislação; e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; 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; A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
	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. 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 ou pelas autoridades administrativas que detenham competência legal para a sua requisição. 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.
Alterações	Alterada pelo Decreto nº 8771/2016 para, entre outras disposições, "indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública"

Decreto nº 10332/2020	**Estratégia de Governo Digital**
Ementa	Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.
Objetivos	Serviços públicos integrados e interoperaráveis, com preenchimento automático de informações;
	políticas públicas baseadas em dados e evidências;
	Serviços públicos do futuro e tecnologias emergentes; implementar recursos de inteligência artificial; disponibilizar dados por meio de soluções de blockchain na administração pública federal; implementar recursos para criação de uma rede blockchain do Governo federal interoperável, com uso de identificação confiável e de algoritmos seguros; implantar um laboratório de experimentação de dados com tecnologias emergentes.
	"Um Governo confiável, que respeita a liberdade e a privacidade dos cidadãos e assegura a resposta adequada aos riscos, ameaças e desafios que surgem com o uso das tecnologias digitais no Estado". Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal e estabelecer método de adequação e conformidade dos órgãos com os requisitos da LGPD; estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020.

Decreto nº 9637/2018	**Política Nacional de Segurança da Informação - PNSI**
Ementa	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.
Princípios	Assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional.
	Respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação; dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas; need to know para o acesso à informação sigilosa; consentimento do proprietário da informação sigilosa recebida de outros países, nos casos dos acordos internacionais.
Objetivos	Os recursos tecnológicos empregados na segurança sistêmica devem apoiar políticas que garantam os princípios fundamentais da autenticidade e da integridade dos dados, e prover mecanismos para proteção da legitimidade contra sua alteração ou eliminação não autorizada. As informações coletadas, processadas e armazenadas na infraestrutura de tecnologia da informação e comunicação devem ser acessíveis apenas a pessoas, a processos ou a entidades autorizadas, a fim de garantir a confidencialidade das informações.

Decreto nº 10046/2019	**Cadastro Base do Cidadão e o Comitê Central de Governança de Dados**
Ementa	Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
Princípios	Nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação.

Fonte: elaborado pela autora a partir do Portal da Legislação (BRASIL, 2020)

O quadro a seguir elenca as aplicações dos eixos selecionados para o projeto BNDES Pilotos IoT, indicando: (i) as soluções relacionadas à coleta, armazenamento, processamento e compartilhamento de dados no âmbito da IoT; (ii) seus impactos na privacidade; (iii) a competência para legislar sobre a matéria em questão, exemplos de legislação aplicável; e (iv) as recomendações de boas práticas.

Quadro 17: Aplicações dos Pilotos IoT: regulação e privacidade

EIXO	APLICAÇÕES (PILOTOS IOT)	IMPACTOS NA PRIVACIDADE	COMPETÊNCIA LEGISLATIVA E REGULATÓRIA	LEGISLAÇÃO APLICÁVEL*	RECOMENDAÇÕES
Pilotos IoT - Cidades Inteligentes					
Mobilidade	Provimento do serviço de veículos elétricos compartilhados.	NA	Federal, estadual e municipal	Código de Trânsito Brasileiro; Conselho Nacional de Trânsito (Contran); Política Nacional de Mobilidade; Estatuto da Cidade	Implementar mecanismos de segurança contra interferência proposital no sinal (anti-jamming) para evitar ataques cibernéticos.
	Controle inteligente da rede semafórica.	NA			
Segurança pública	Implantação de câmeras e visão computacional para segurança pública.	Tecnologias como videomonitoramento, reconhecimento facial e captação sonora aumentam a eficiência da segurança pública, mas têm potencial direto de impacto na privacidade.	Federal e estadual (acesso e tratamento dos dados) e municipal (instalação dos equipamentos, além de acesso e tratamento dos dados)	Constituição Federal; Lei Geral de Proteçao de Dados; Código de Processo Civil e Código de Processo Penal; Marco Civil da Internet; Política Nacional de Segurança da Informação	Observar os limites e controles necessários para evitar abusos por parte do Estado. O tratamento de dado pessoal sensível deve obedecer aos princípios da finalidade e proporcionalidade, e ser realizado por autoridades competentes, sendo estritamente observadas as políticas de acesso aos dados por terceiros ou cessão para outras entidades, além da necessidade de ordem judicial para casos que extrapolem a motivação inicial de coleta.
	Integração com videomonitoramento para segurança pública.				
	Implantação de rede com videomonitoramento para segurança pública, defesa civil e parquímetros eletrônicos.				
	Monitoramento de situações de crime e ameaças à segurança urbana.				

Eficiência energética	Medição de microclima na área urbana.	NA	Os postes (infraestrutura central para IoT em cidades) podem ser ativos de iluminação pública (municípios) ou os ativos de energia elétrica (União), estes últimos utilizados também para telecomunicações.	Resoluções e normas da Aneel, Anatel, Agência Nacional do Petróleo, além das regulamentações locais dos municípios e das respectivas concessionárias.	Adotar técnicas de anonimização de dados, por criptografia ou blockchain, para armazenar de forma segura e a longo prazo informações detalhadas. A coleta de dados por medidores inteligentes ou qualquer outro dispositivo de IoT na rede elétrica seve ser feita apenas para a finalidade de medição do consumo e gestão da rede, exceto com consentimento livre, expresso e informado dos usuários ou determinações legais.
	Implantação de plataforma completa de telegestão para iluminação publica.	A integração de smart grids com câmeras de segurança podem comprometer a privacidade, se forem coletados dados sensíveis. O acesso às informações de consumo de energia elétrica de indivíduos permite monitoramento de padrões comportamentais, fraudes nos valores da fatura do usuário (por falhas de segurança), perfilamento, envio de publicidade não desejada etc.			
	Implantação de telegestão na rede de iluminação inteligente (*smart grid*).				
	Implantação de rede de iluminação pública habilitadora de soluções de IoT, tais como lixeiras inteligentes.				
	Implantação de redes de iluminação pública habilitadoras de soluções de IoT.				

* Não exaustiva

Fonte: elaborado pela autora a partir de informações do BNDES (2018b) e do Portal da Legislação (BRASIL, 2020)

5.4.2. Impacto regulatório

A Anatel realizou Análise de Impacto Regulatório (AIR) com o objetivo de reavaliar “a regulamentação visando diminuir barreiras regulatórias à expansão das aplicações de internet das coisas e comunicações máquina-a-máquina, tais como regras de qualidade, licenciamento, atendimento, dentre outros”. A análise foi aprovada pela Portaria Anatel nº 1, de 2 de janeiro de 2018, e contou com a participação de diversos atores interessados, conforme consta do relatório da Anatel (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL), 2019).

A análise identificou sete eixos, divididos em problemas, temas e alternativas, dos quais foram selecionados os mais diretamente ligados à questão da privacidade e apresentados resumidamente a seguir. As alternativas sugeridas pela Anatel para cada tema encontram-se grifadas, fundamentadas no Relatório de AIR. Como conclusão da análise, a agência propôs “a realização de Consulta Pública acerca da reavaliação da regulamentação visando diminuir barreiras regulatórias à expansão das aplicações de internet das coisas e comunicações máquina-a-máquina”. (BRASIL, 2019c)

Quadro 18: Análise de Impacto Regulatório - Anatel

E1: OUTORGA	
E1.T2: Transparência com o regulado	
Problema	Há incerteza ou falta de clareza quanto à outorga adequada para cada modelo de negócio envolvendo IoT.
Objetivos	Aumentar a transparência dos regramentos vigentes relativamente às questões que impactam a IoT, no sentido de que as possibilidades trazidas pela regulamentação fiquem claras a qualquer interessado.
Alternativas	Alternativa A – Aumentar a transparência dos regramentos vigentes relativamente às questões que impactam a IoT, no sentido de que as possibilidades trazidas pela regulamentação fiquem claras a qualquer interessado.
	Alternativa B – Aprimorar as informações disponíveis na página da Anatel na Internet acerca dos serviços de telecomunicações existentes.
	Alternativa C – Publicar cartilha orientativa, explicando as principais possibilidades regulatórias para viabilizar aplicações IoT/M2M
E2.T2: Direitos do consumidor e obrigações de qualidade aplicáveis ao ecossistema IoT	
Problema	Algumas obrigações do SMP e do SCM, especialmente as que envolvem direitos do consumidor e qualidade, não foram modeladas ou não se mostram adequadas para o cenário de IoT/M2M.
Objetivos	Conciliar o desenvolvimento de aplicações IoT/M2M com o resguardo dos direitos do consumidor e respeito às obrigações de qualidade.
Alternativas	Alternativa A – Manter o cenário atual.
	Alternativa B – Inserir regras específicas e diferenciadas para tais serviços quando explorados em aplicações IoT/M2M nas atuais revisões do modelo de qualidade (RGQ) e da regulamentação consumerista (o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC).
	Alternativa C – Excluir as obrigações relativas à qualidade e aos direitos do consumidor no SMP e SCM quando a sua exploração envolver aplicações IoT (tais obrigações seriam reguladas contratualmente).
	Alternativa D – Criar regras específicas e diferenciadas para tais serviços quando explorados em aplicações IoT/M2M em normativo próprio.

E5: AVALIAÇÃO DE CONFORMIDADE	
E5.T1: Demanda de avaliação da conformidade de produtos IoT	
Problema	Risco de o volume massivo de solicitações para homologação de produtos gerar um gargalo na autorização do uso e comercialização de produtos IoT/M2M.
Objetivos	Permitir a introdução de dispositivos IoT aderentes aos requisitos técnicos estabelecidos pela Agência no País, sem que o processo de avaliação de conformidade se torne um gargalo na disponibilização dos dispositivos ao mercado.
Alternativas	Alternativa A – Não realizar a avaliação da conformidade de dispositivos IoT/M2M.
	Alternativa B – Alterar a avaliação da conformidade de dispositivos IoT/M2M para Declaração de Conformidade.
	Alternativa C – Manter o processo vigente.
E5.T2: Segurança cibernética em dispositivos IoT	
Problema	Presença de vulnerabilidades de segurança em produtos para telecomunicações, mais especificamente em dispositivos IoT/M2M, conectados à rede mundial de informação (internet), que propicia, entre outros, a proliferação de ataques cibernéticos.
Objetivos	Identificar e proporcionar ao consumidor um ambiente com maior segurança cibernética. Aí se incluem a estabilidade e a confiabilidade. O objetivo imediato é mitigar a probabilidade de ocorrência de ataques cibernéticos que explorem vulnerabilidades existentes em dispositivos IoT.
Alternativas	Verificou-se que, para o presente tema, o problema a ser atacado, assim como as alternativas aventadas estão sendo endereçados no item 58 da Agenda Regulatória 2017-2018, referente à revisão da regulamentação sobre segurança das redes de telecomunicações (Processo nº 53500.078752/2017-68).
E7: INFRAESTRUTURA E INSUMOS	
E7.T3: Compartilhamento de Infraestrutura	
Problema	Dificuldade de acesso a infraestruturas passivas para ampliação das redes de telecomunicações (disponibilidade e preços).
Objetivos	Facilitar a ampliação de redes de telecomunicações de acesso promovendo o compartilhamento de infraestrutura dentro do setor de telecomunicações ou com o setor de energia elétrica, especialmente da rede de distribuição deste serviço.
Alternativas	Verificou-se que, para o presente tema, existem dois projetos na Agência que permeiam o tema, a saber, os itens nº 2 e 61 da Agenda Regulatória para o biênio de 2017 e 2018. Quanto ao primeiro item, em outubro de 2017, foi publicada a Resolução nº 683, que aprovou o Regulamento de Compartilhamento de Infraestrutura de Suporte à Prestação de Serviço de Telecomunicações. Em relação ao segundo item, trata-se do projeto de reavaliação da regulamentação sobre compartilhamento de postes entre distribuidoras de energia elétrica e prestadoras de serviços de telecomunicações, o qual se encontra na etapa de elaboração de Análise de Impacto Regulatório.

Fonte: adaptado de ANATEL (2018).

5.5. Impacto orçamentário e financeiro

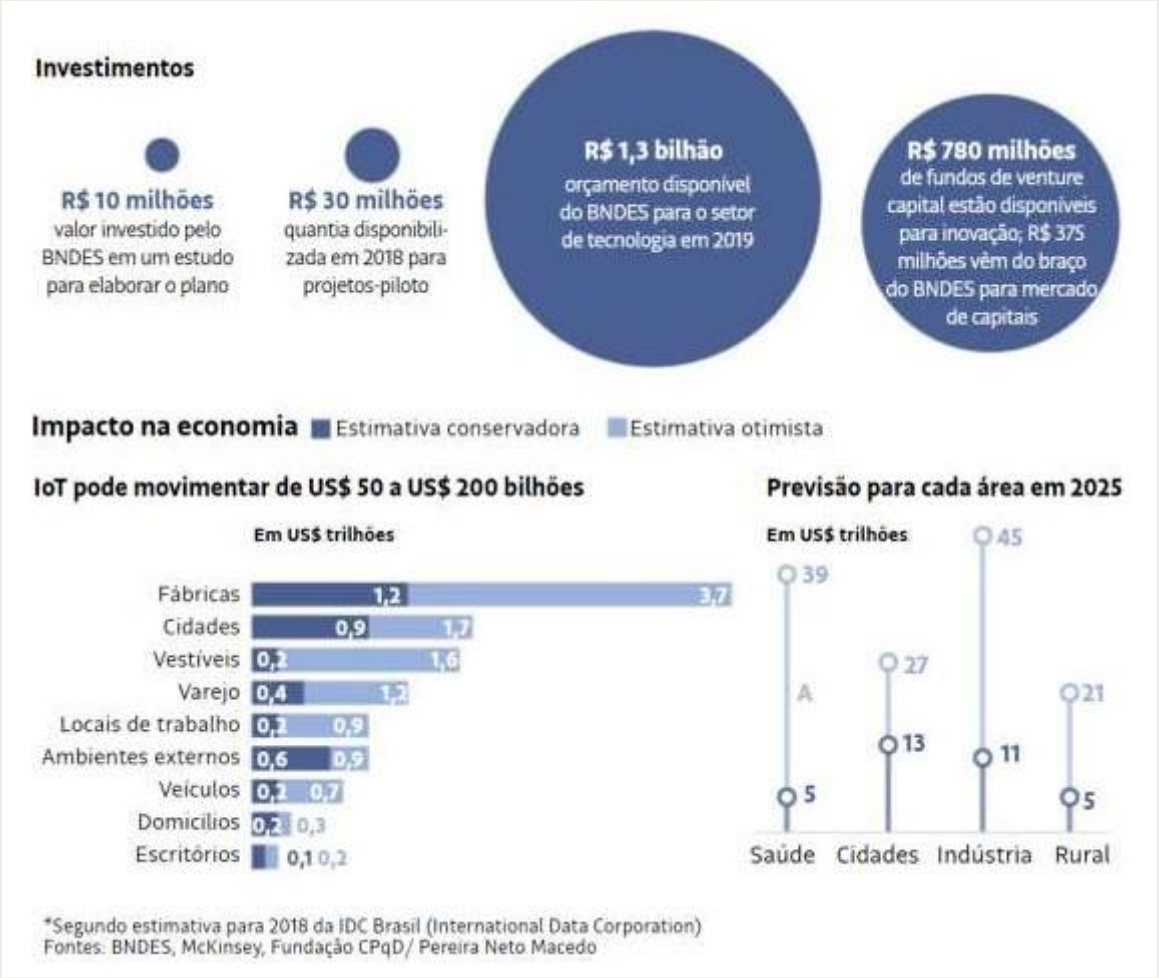
Neste tópico, toma-se a expressão “impacto orçamentário” em sentido amplo, tendo em vista que os financiamentos concedidos pelo BNDES não integram a lei orçamentária anual da União e, portanto, são de natureza extraorçamentária.

Conforme mencionado, as redes de fomento em nível nacional com recursos voltados para investimentos em IoT identificadas foram:

- BNDES: investiu por volta de R$ 10 milhões no estudo que subsidiou o Plano Nacional de IoT (BNDES, 2017d); programou investimentos de R$ 30 milhões não reembolsáveis no programa Pilotos IoT (BNDES, 2018a), dos quais foram executados R$ 7 milhões, conforme apresentado na tabela do modelo lógico (item 5.3.3), em valores extraídos do sistema “Consulta a operações do BNDES” (Anexo 2); criou o Fundo de Investimento em Participações (FIP) em Internet das Coisas (IoT) via BNDESPAR, sociedade de participações acionárias do banco, em parceria público-privada com a empresa Qualcomm Ventures de telecomunicações (BNDES, 2019), com a previsão de aporte de até R$ 40 milhões, com o limite de até 25% do capital comprometido total do fundo, por cada uma das parceiras; além de destinar outros recursos para o setor de tecnologia e inovação que podem ser aplicados em IoT;
- Finep: lançou em junho de 2018 programa de investimentos de R$ 1,5 bilhão, com financiamento reembolsável para projetos de Internet das Coisas (Finep IoT), sendo a maior parte dos recursos (R$ 1,1 bilhão) da própria Finep, somados a R$ 400 milhões do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel) (FINEP, 2018); e
- Embrapii: disponibilizou em julho de 2019 R$ 8 milhões em recursos não reembolsáveis para projetos de inovação em IoT e Manufatura 4.0 (EMBRAPII, 2019).

O infográfico da Folha de São Paulo (2019) a seguir apresenta uma visão geral dos investimentos previstos para o setor e dos impactos projetados na economia.

Figura 16: Fomento ao ecossistema de IoT



Fonte: Folha de São Paulo (2019)

5.6. Estratégias de construção de confiança e suporte da política

Conforme o Guia Prático de Análise *Ex Ante* (2018), as estratégias de construção de confiança e suporte da política envolvem o estabelecimento de confiança pública, dada pela percepção de relevância do problema da política para o interesse coletivo e pela confiança na capacidade das instituições para implementá-la. No caso do Plano Nacional de IoT, pelo exposto em seções anteriores, resta claro o potencial de melhoria da qualidade de vida da população pelas tecnologias de IoT nos ambientes priorizados. Esse potencial pôde ser reconhecido nos fóruns de coparticipação para a construção das aspirações de IoT para o país, que fundamentaram o Plano.

O envolvimento dos interessados é demonstrado pela participação efetiva de diversos atores envolvidos com a política, inclusive a sociedade civil, conforme

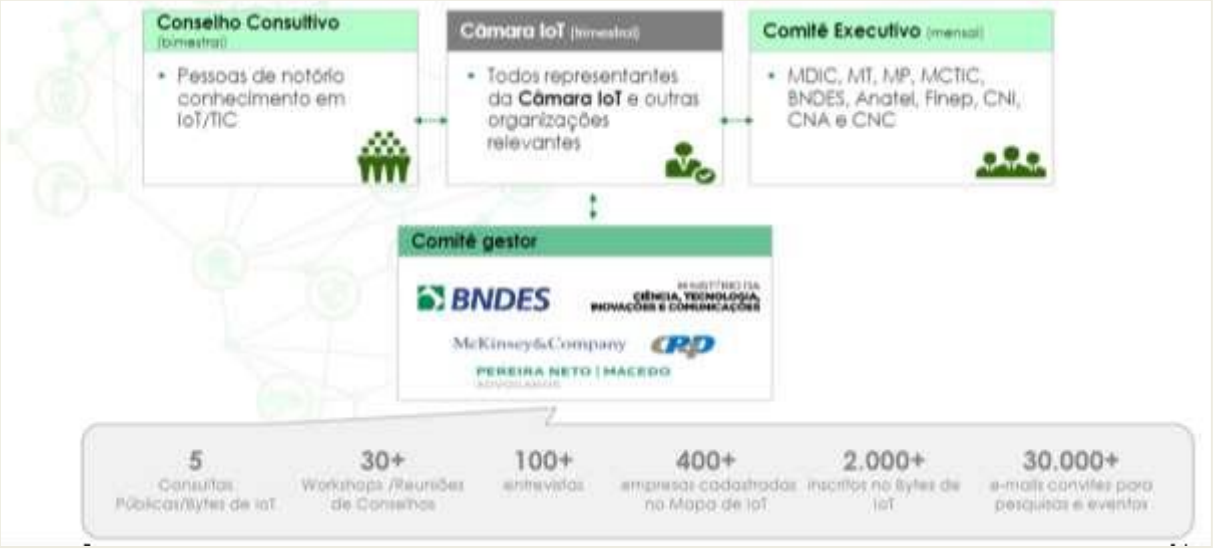
relatado na seção 5.3.2 e sumarizado no infográfico a seguir. O processo de construção colaborativa do plano de ação, ilustrado anteriormente na Quadro 6: Fases e produtos do plano de ação de IoT, indica a entrega de relatórios da entrevistas, que permearam três das quatro fases do estudo (BNDES, 2017d). Foram realizadas ainda consultas públicas e eventos sobre o tema, com participações resumidas abaixo.

Figura 17: Engajamento na construção do Plano de Ação para IoT

Fonte: BNDES (2017d)

Dados extraídos das consultas indicam a percepção dos benefícios da IoT para aumento da competitividade da economia e melhoria da qualidade de vida dos cidadãos. Foi identificada também uma aspiração sobre a possibilidade de destaque do Brasil na América Latina ou em verticais como o agronegócio. As reflexões foram discutidas no evento Laboratórios do Futuro. As instâncias de governança do ecossistema de IoT, como Câmara IoT, Comitê Executivo e Conselho Consultivo, foram amplamente representadas e engajadas nas discussões, conforme esquema a seguir. As contribuições foram sintetizadas e priorizadas nas diversas reuniões de governança do estudo (BNDES, 2017d).

Figura 18: Interlocução com atores chaves para construção da proposta de IoT



Fonte: BNDES (2017d)

O quadro a seguir apresenta um resumo das demandas de diferentes atores do ecossistema de IoT, incluindo iniciativa privada, academia e investidores.

Quadro 19: Demandas dos atores para acompanhamento do Plano de IoT

Relação entre funcionalidades levantadas e demandas dos usuários

✓ Necessidade principal do ator
✓ Necessidade secundária do ator

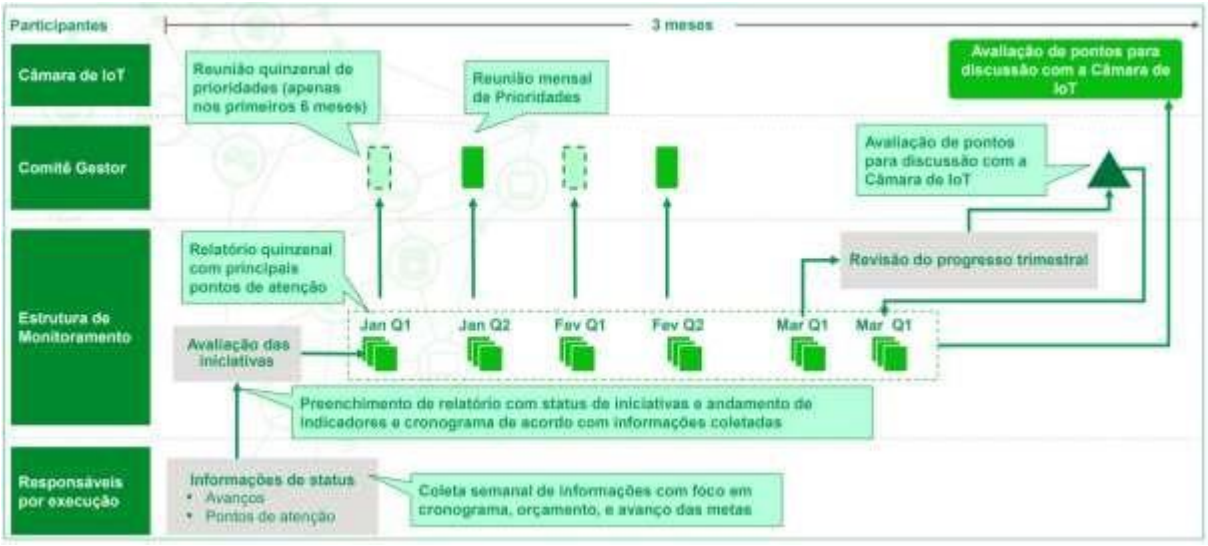
		Mercado Privado	Academia & Pesquisa	Investidores
Status do plano	• Acompanhamento da evolução das iniciativas do plano			✓
Repositório de informações relevantes para IoT	• Repositório de artigos nacionais e internacionais criados sobre IoT		✓	
	• Repositório de profissionais e acadêmicos do Brasil e do mundo capacitados em IoT	✓	✓	✓
	• Repositório de eventos organizados por parceiros relacionados ao tema de IoT	✓	✓	✓
Mapeamento e atualização de temas gerais relevantes para IoT	• Banco de informações atualizado dos instrumentos de financiamento para IoT	✓	✓	✓
	• Mapeamento atualizado das empresas relacionadas a IoT no contexto local e no mundo, com possibilidade de segmentação das mesmas por critérios relevantes aos usuários (p.ex.: Porte da empresa, segmento da cadeia de produção que atua entre outros)	✓	✓	✓
	• Mapeamento de cursos online e de ensino superior para ofertantes e demandantes de IoT	✓	✓	
	• Mapeamento de marcos legais relacionados a IoT com seu status atual de evolução	✓	✓	✓
	• Cadastro de novas startups e think tanks ligadas ao tema	✓		✓
Levantamento do panorama de IoT	• Mapeamento atualizado de informações gerais sobre IoT no contexto local (número total de empresas, funding, elos da cadeia mais valorizados, total de cursos voltados ao tema na academia)	✓	✓	
Mapeamentos de temas específicos referentes a IoT	• Mapeamento de ICTs, test beds e projetos pilotos relacionadas a IoT	✓	✓	
	• Mapeamento das regiões com maior potencial de se tornarem polos regionais de desenvolvimento tecnológico em IoT no Observatório			
	• Casos de sucesso em relação ao uso de IoT no Brasil e no mundo		✓	
Comparativos	• Criação de ranking público de produtividade de ICTs	✓		
	• Busca de conexões *peer to peer* regionalizada de empresas e atores da indústria de IoT	✓	✓	✓
Organização e participação em Eventos	• Organização de eventos nacionais e internacionais relacionados a IoT, com *stakeholders* relevantes para os temas estratégicos para o plano			
	• Participação em eventos relacionados ao tema	✓	✓	✓
Geração de conhecimento de vanguarda em IoT	• Pesquisa e publicação de relatórios sobre temas específicos para IoT		✓	
	• Desenvolvimento de plataformas e programas educacionais		✓	

Fonte: BNDES (2017d)

5.7. Monitoramento, avaliação e controle da política

O estudo do BNDES sugeriu a estrutura de monitoramento ilustrada na imagem a seguir (BNDES, 2017d).

Figura 19: Estrutura de monitoramento do Plano Nacional de IoT



Fonte: BNDES (2017d)

A Câmara IoT, presidida pelo MCTIC, tem como objetivo “acompanhar a evolução e o surgimento de novas aplicações máquina a máquina e Internet das Coisas; subsidiar a formulação de políticas públicas que estimulem o desenvolvimento de sistemas máquina a máquina e Internet das Coisas; e promover e coordenar a cooperação técnica entre todos os atores que fazem parte do ecossistema de Internet das Coisas no Brasil”. Portanto, foi regulamentada no decreto do Plano Nacional de IoT (BRASIL, 2019a) para cumprir a função idealizada no modelo de monitoramento do estudo que o subsidiou (BNDES, 2017d). Todavia, na data da consulta deste trabalho (junho/2020), a página do portal do MCTIC dedicada à IoT não apresentava nenhuma informação, conforme figura a seguir.

Figura 20: Página do MCTIC sobre a política de IoT

Fonte: MCTIC (2020a)

Outro instrumento de monitoramento, avaliação e controle da política instituído pelo decreto do Plano de IoT (BRASIL, 2019a) foi o “Observatório Nacional para o Acompanhamento da Transformação Digital”, lançado pelo MCTIC em parceria com o Movimento Brasil Competitivo e o CPqD. O Movimento Brasil Competitivo, conforme declara sua missão, promove debates e ações para a transformação do país nas áreas de economia digital e reforma do Estado, além de coordenar a coalizão Brasil Digital, com mais de 25 empresas interessadas nas referidas áreas. O CPqD, por sua vez, é uma organização privada orientada à inovação, tecnologia e transformação digital. O Observatório constitui-se, portanto, de uma parceria entre sociedade civil, iniciativa privada e governo federal, que busca “garantir o engajamento e a participação efetiva dos cidadãos brasileiros no acompanhamento das políticas públicas sobre o tema no país” (OBSERVATÓRIO DA TRANSFORMAÇÃO DIGITAL, 2018b).

A criação do Observatório também foi idealizada pelo estudo do BNDES (2017d), em um modelo detalhado, apresentado como “Observatório de IoT”. Na prática, acabou tomando uma proporção mais ampla, abarcando ferramentas para acompanhamento e monitoramento das ações de políticas públicas relacionadas à economia digital em geral em curso no país, dentre as quais o Plano Nacional de IoT.

O estudo do BNDES (2017d) indicava a necessidade de formulação de indicadores para acompanhamento das ações do Plano Nacional de IoT, dentre os quais: indicadores de esforço, que refletem o avanço das iniciativas; e indicadores de impacto, que refletem os resultados finais para a sociedade. Outra premissa do Observatório seria a de funcionar como instrumento de organização de informações e de transparência, apresentando em uma plataforma centralizada “os mecanismos de apoio à empresa que demanda e que oferta soluções de IoT, seja por financiamento, cursos de capacitação ou parceria com instituições de ensino para pesquisa e desenvolvimento”. Atualmente, por exemplo, para buscar financiamento é preciso consultar as diversas linhas elencadas na seção 5.5 (BNDES, Finep e Embrapii). Entretanto, ao consultar o portal do Observatório, a última atualização é de 2018.

Figura 21: Página do Observatório da Transformação Digital

Fonte: Observatório da Transformação Digital (2018b)

O quadro a seguir apresenta o acompanhamento das ações do plano realizado pelo Observatório, com destaque para a ação 45, que trata de privacidade, foco deste trabalho. A ação está concluída, na medida em que a “autoridade central independente para a proteção e segurança de dados pessoais” foi definida no âmbito da LGPD (BRASIL, 2018a). O portal está, portanto, desatualizado. Foi encaminhada uma mensagem ao formulário de contato, porém, sem retorno até a data de finalização deste trabalho.

Quadro 20: Plano de ação para IoT: Regulatório, Segurança e Privacidade

LEGENDA	○ EM PREPARAÇÃO	◐ EM ANDAMENTO	● CONCLUÍDA

AÇÃO	HORIZONTAL	DESCRIÇÃO	STATUS
43	Regulatório, Segurança e Privacidade	Realizar mapeamento do uso do espectro licenciado no Brasil, fazendo uso da previsão contida no art. 5º, I, da Resolução Anatel nº 671, de 3 de novembro de 2016.	○
44	Regulatório, Segurança e Privacidade	Revisar os requisitos técnicos previstos na regulamentação para a avaliação da conformidade de equipamentos de radiocomunicação restrita, de modo a evitar barreiras de entrada a tecnologias específicas.	○
45	Regulatório, Segurança e Privacidade	Definir autoridade central independente para a proteção e segurança de dados pessoais, potencialmente em modelo de co-regulação.	○
46	Regulatório, Segurança e Privacidade	Estruturar governança baseada em modelo multissetorial, com a criação ou designação de estrutura específica para a coordenação de atividades baseadas em segurança da informação, na forma de conselho permanente, órgão/entidade pública ou agência reguladora independente.	○
47	Regulatório, Segurança e Privacidade	Estimular a cooperação e interação entre o Poder Público, sociedade civil, iniciativa privada e academia, com o fim de promover medidas de conscientização e fomento da segurança da informação.	○
48	Regulatório, Segurança e Privacidade	Aprimorar os mecanismos de cooperação internacional para a prevenção e tratamento de incidentes de segurança da informação, como pela adesão a Acordos de Troca e Proteção Mútua de Informações Classificadas.	○
49	Regulatório, Segurança e Privacidade	Incentivar a adoção de padrões internacionais na temática de segurança da informação pela iniciativa privada.	○
50	Regulatório, Segurança e Privacidade	Incentivar a criação de sistema de certificação creditatória de segurança da informação em dispositivos em Internet das Coisas, baseada em modelo de autorregulação voluntária pela iniciativa privada.	○
51	Regulatório, Segurança e Privacidade	Fortalecer a estrutura institucional dedicada à segurança de infraestruturas críticas no âmbito da Administração Pública Federal, e incentivar os setores regulados a respeitarem aspectos mínimos de segurança da informação, em particular em setores de infraestrutura crítica.	○

Fonte: adaptado de Observatório da Transformação Digital (2018b)

6. Análise crítica

Para proceder à análise crítica do Plano Nacional de IoT, foi utilizado como base o Referencial para Avaliação de Governança em Políticas Públicas do TCU (2014), segundo o qual “governança em políticas públicas se refere aos arranjos institucionais que condicionam a forma pela qual as políticas são formuladas, implementadas e avaliadas, em benefício da sociedade” (BRASIL, 2014, p. 32).

A análise contempla os oito componentes do modelo adotado, detalhados de forma resumida a seguir, juntamente com os respectivos aspectos da política avaliados. Cabe ressaltar que este trabalho não se pretende exaustivo, contempla apenas alguns aspectos do objeto de estudo, que é complexo e multifacetado.

Figura 22: Modelo de Avaliação de Governança em Políticas Públicas

Fonte: adaptado de Brasil (2014)

(I) Institucionalização

Este componente avalia a formalização da política, que lhe confere legitimidade. O Plano Nacional de IoT cumpre esse papel, na medida em que foi instituído pelo Decreto 9.854/2019 (BRASIL, 2019a), e subsidiado por amplos estudos (BNDES, 2017d), conforme detalhado nas seções 5.2 e 5.3.3. Entretanto, pelo

observado no decorrer do trabalho, existem lacunas em regulamentações subsidiárias, abordadas no item II, dada a sobreposição dos componentes indicada no próprio Referencial (BRASIL, 2014, p. 17).

Weber (2013) defende a necessidade de novas abordagens regulatórias para garantir privacidade e segurança na IoT. Segundo ele, a natureza da IoT pede um quadro jurídico heterogêneo e diferenciado, que tome devidamente em conta sua globalidade, verticalidade, onipresença e tecnicidade. Legislações geograficamente limitadas não parecem adequadas neste contexto. No entanto, a autorregulação que tem sido aplicada até agora pode não ser suficiente para garantir proteções eficazes. Um referencial de princípios fundamentais estabelecidos por um legislador internacional, complementado pelo setor privado com uma regulamentação mais detalhada, parece ser a melhor solução. A inclusão de um legislador internacional no processo garante o envolvimento contínuo do setor público, que pode contribuir no mínimo com o monitoramento do processo (LACERDA, 2015).

(II) Planos e objetivos

Este critério é relativo à coesão interna de objetivos e metas. O plano de ação (BNDES, 2017) e a E-digital (2018a) são instrumentos que detalham a estratégia de implantação da IoT de forma consistente, de acordo com o descrito na seção 5.2. Mas há que se garantir que as inovações estejam de acordo com o interesse público. Nesse sentido, ao analisar as ações do plano relativas à vertical cidades inteligentes e sua interrelação com a horizontal privacidade, apresentam-se a seguir alguns pontos considerados relevantes para o debate proposto por este trabalho.

Em termos de garantia de privacidade, houve um grande avanço no Brasil com a aprovação da LGPD (BRASIL, 2018a) como marco legal para a proteção de dados, pautada em princípios de interesse público, finalidade, necessidade, transparência, consentimento, direito de retificação, dentre outros. A norma unifica mais de 40 estatutos que regem dados pessoais (KOCH, 2019), em consonância com a *General Data Protection Regulation* (GDPR), que regulamenta a privacidade na União Europeia. A lei traz ainda relevantes alterações ao Marco Civil da Internet (BRASIL, 2014), com a possibilidade de exclusão definitiva de dados pessoais fornecidos a aplicativos ou considerados excessivos em relação à finalidade original pelo titular, ressalvadas as hipóteses legais.

A instituição da Autoridade Nacional de Proteção de Dados para assegurar o cumprimento da lei foi também um passo fundamental em direção à garantia dos direitos de privacidade. Entretanto, vale ressaltar que aplicações de IoT já estão implantadas em diversas cidades do país, e a vigência da LGPD só se inicia, em princípio, em agosto de 2020, sendo que as sanções só entrarão em vigor em agosto de 2021, conforme prorrogação pela Lei nº 14.010/2020 (BRASIL, 2020e), ocorrida em função da crise de saúde pública causada pela Covid-19. Esse prazo pode ainda ser alterado pela Medida Provisória 959 (BRASIL, 2020c), que tramita no Congresso Nacional, e prorroga o início da vigência da LGPD para maio de 2021, caso convertida em lei. Além disso, a implantação efetiva da Autoridade Nacional encontra entraves políticos e operacionais, trazendo um contexto de insegurança jurídica na aplicação da LGPD.

Almeida, Filgueiras e Gaetani (2019) estabelecem a conformidade com padrões e regulamentos para proteção de dados como um princípio para a governança de serviços públicos digitais, para garantir a confiança dos usuários nas soluções e evitar o uso indevido dos dados para finalidades comerciais, políticas ou sociais. Ressaltam ainda o papel dos agentes reguladores nesse contexto.

Nesse sentido, tem sido questionado o Decreto 10.046/2019 (BRASIL, 2019d), que regulamenta o compartilhamento de dados entre órgãos públicos federais, ampliando o escopo dos dados intercambiáveis ao incluir “atributos biográficos e biométricos” produzidos e coletados no âmbito da execução de políticas públicas. As ressalvas são feitas em função da possibilidade de compartilhamento de dados classificados como sensíveis, sem a devida observância a princípios estabelecidos pela LGPD, como finalidade, necessidade e transparência por parte do governo; e prerrogativas do cidadão ao livre acesso, consentimento do titular, autodeterminação informativa, entre outros.

No intuito de simplificar e desburocratizar o intercâmbio e o cruzamento das bases pelo governo, em prol da eficiência da gestão pública, o decreto falha, segundo os críticos, em prever limites, regras e salvaguardas que garantam a proteção e a segurança dos dados dos cidadãos. Os riscos incluem, por exemplo, a possibilidade de uso de perfilamento (modelos construídos a partir de grandes quantidades de dados utilizados para inferências), abrindo brechas para práticas discriminatórias, de vigilância e de controle sem causa justificável, como o policiamento preditivo, com exemplos ilustrados na pesquisa de Babuta e Oswald (2019). O decreto está sendo

contestado em três Projetos de Decreto Legislativo (PDLs), que pretendem sustar seus efeitos: PDL 661/2019, PDL 675/2019 e PDL 673/2019 (FRAGOSO; MASSARO, 2019). Em ação recente ajuizada junto ao Supremo Tribunal Federal (STF), o Partido Socialista Brasileiro (PSB) pediu a suspensão do compartilhamento de dados da Carteira Nacional de Habilitação (CNH) pelo Serviço Federal de Processamento de Dados (Serpro) com a Agência Brasileira de Inteligência (Abin), questionando os princípios da finalidade, da transparência e do consentimento pelos titulares. Segundo o Ministro Gilmar Mendes, relator do caso:

> O regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea. Por esse motivo, é dever constitucional deste STF debruçar-se sobre a matéria, evitando-se que situações graves que colocam em risco a violação de preceitos fundamentais sejam perpetradas com suposto fundamento no Decreto nº. 10.046, de 9 de outubro de 2019. Destaca-se ainda que a presente decisão não obsta a eventual análise de medida acauteladora relacionada à alegações de inconstitucionalidade deste ato normativo (MENDES, 2020).

No que tange à segurança pública nas cidades, cabe ao Estado garanti-la por meio da execução de políticas públicas eficientes (CF art. 144); portanto, é permitido implementar mecanismos de vigilância por aplicações de IoT. Mas tecnologias como videomonitoramento, reconhecimento facial e captação sonora têm potencial de atingir direitos fundamentais como privacidade e liberdade de expressão. Há que se observar os limites e controles necessários para evitar abusos por parte do Estado, como práticas discriminatórias, policiamento preditivo ou falsa identificação de pessoas com criminosos devido a falhas nos sistemas, além de ameaças à democracia, como desestimulo a manifestações públicas (*chilling effect*), muitos dos quais exemplos de situações reais (BNDES, 2017d; BURGESS, 2018; DW BRASIL, 2017; GRIERSON, 2019).

A título de ilustração, em 2017 um sistema de reconhecimento facial utilizado na UEFA Champions League classificou 2.470 pessoas como criminosas, sendo que apenas 173 foram corretamente identificadas, ou seja, um índice de 92% de erro (BURGESS, 2018). As autoridades brasileiras testaram um sistema durante o Carnaval de 2019 com um índice de falhas similar, de 90%, de acordo com a Coding Rights. O sistema utilizado no metrô do Rio de Janeiro também falhou no primeiro dia, levando uma cidadã por equívoco à delegacia pelas autoridades. O que agrava os

percentuais de erro são os eventuais vieses e preconceitos cometidos pelos “algoritmos”. É o caso de um casal de negros que teve uma foto sua classificada como “gorilas” pelo Google Images em 2015 (TAUTE, 2020). Os erros são dez vezes mais frequentes com mulheres negras do que com brancas, segundo o *National Institute of Standards and Technology*, e a precisão de identificação em geral é menor em peles mais escuras (DW BRASIL, 2017; TAUTE, 2020), o que pode agravar um problema que já é flagrante na sociedade, o de violência policial e racismo, que motivou recente debate nas Nações Unidas, dentre muitos outros fóruns (GONÇALVES; GONÇALVES, 2020; UNITED NATIONS, 2020).

A tendência é que a acurácia das soluções seja cada vez maior com a evolução tecnológica. Ainda assim, há que se questionar as bases éticas do uso dessas ferramentas pelo poder público e suas consequências para os cidadãos, garantindo a preservação dos direitos fundamentais a partir de um sistema de freios e contrapesos. Nesse sentido, o Fórum Europeu para a Segurança Urbana publicou a “Carta de Uso Democrático da Videovigilância” (EFUS, 2010) com sete princípios norteadores para o uso dessa tecnologia para segurança pública: legalidade, necessidade, proporcionalidade, transparência, responsabilidade, supervisão independente e participação (implicação) dos cidadãos. O Fórum publicou posteriormente o “Manifesto: Segurança, Democracia e Cidades: coproduzir as políticas de segurança”, que trata mais especificamente da participação ampla e ativa do cidadão na concepção, implementação e avaliação das políticas de segurança (EFUS, 2018).

É possível listar inúmeros casos que justifiquem a preocupação com o limite da atuação do Estado no sentido de manter a inviolabilidade da privacidade e as liberdades civis. Faz-se necessária a busca constante de equilíbrio entre privacidade e segurança, para garantia da qualidade de vida sem ameaças à democracia. Uma analogia recorrente na literatura especializada é o “efeito panóptico”, explorado na obra “Vigiar e Punir”, de Michel Foucault (2014). O panóptico seria uma espécie de penitenciaria ideal, idealizada por Jeremy Bentham em 1785, com um ponto central, de onde o observador a todos se vê, mas não pode ser visto. “Quanto mais uma cidade pode medir e controlar, maior a probabilidade de se tornar "panóptica", capaz de rastrear tudo, nunca esquecendo o que acontece. Em outras palavras, um tipo de sociedade do Big Brother” (NEWCOMBE, 2014). A perspectiva distópica, embora muitas vezes alegórica, é útil para enfatizar os limites das políticas públicas.

Em síntese, o estudo do BNDES (2017d) elenca como iniciativas para coleta, tratamento e compartilhamento de dados na implementação das ações do Plano Nacional de IoT: publicação de um marco legal específico, requisito cumprido pela LGPD (BRASIL, 2018a); dispensabilidade de consentimento prévio para dados pessoais necessários à prestação de serviços públicos essenciais (*opt-in)*; respeito ao princípio da finalidade na coleta do dado; existência de mecanismos de descadastramento (*opt-out*) para o usuário do serviço; adoção de técnicas de anonimização e agregação de dados; vedação ao compartilhamento de dados com terceiros, exceto se anonimizados ou no caso de consentimento livre, expresso e informado ou de determinação judicial. Além disso, é recomendada a elaboração de guia de boas práticas, na linha do *Data Protection Impact Assessment* - DPIA, utilizado no escopo da GDPR (EUROPEAN UNION, 2018), com a indicação de políticas, diretrizes e procedimentos para garantir a gestão de riscos de privacidade nas soluções de IoT.

Nessa linha, diversos autores recomendam a prática de tratar a privacidade desde a concepção (*privacy by design*), na qual as soluções já são desenvolvidas de forma compatível com os princípios proteção de dados pessoais, incluindo técnicas de anonimização, como criptografia e privacidade diferencial, que evitam a identificação e a inferência de informações. Essa abordagem minimiza a necessidade de ajustes futuros, que podem ser custosos ou até inviáveis (BNDES, 2017b; HUSTINX, 2010).

As soluções da vertical cidades inteligentes voltadas para mobilidade urbana e eficiência energética apresentam problemas indiretos relacionados à privacidade, especialmente quando há integração com soluções de segurança pública, conforme detalhado no Modelo lógico. Outro ponto é a segurança da informação nos dispositivos, sujeitos a vazamentos e obtenção ilegal de dados. Sobre o assunto, o Acórdão 1613/2020 – Plenário, do TCU (2020) recomenda o uso da tecnologia *blockchain*.

> Na IoT, independente do setor da economia, a tecnologia *blockchain* pode proporcionar uma forma de rastrear a história única de cada dispositivo, registrando a troca de dados entre ele e outros dispositivos, serviços web e usuários humanos. Pode também permitir que dispositivos inteligentes se tornem agentes independentes que conduzem de forma autônoma uma variedade de transações (BRASIL, 2020).

Sobre o desenho e a implementação da política, há que se considerar que o Brasil tem dimensões continentais e especificidades regionais em termos de cidades. As soluções devem ser pensadas de forma contextualizada, para garantir uma política equitativa e inclusiva, atendendo às necessidades dos cidadãos (KNOPIK, 2018)

(III) Participação

Este componente avalia a participação da sociedade e dos atores interessados nos processos decisórios da política pública. A elaboração do Plano Nacional de IoT e os estudos e estratégias que o subsidiaram envolveram uma série de chamadas públicas e estudos com grupos representativos, conforme detalhado na seção 5.6. Ao que tudo indica, os múltiplos atores foram envolvidos nas discussões.

Jane Jacobs, em “Morte e vida de grandes cidades”, originalmente publicado em 1961, declara que "as cidades têm a capacidade de prover algo para todos, somente porque, e somente quando, são criadas por todos", e, ainda, que “não existe uma lógica que possa ser sobreposta à cidade; as pessoas fazem a lógica, e é em favor delas, e não dos edifícios, que devemos moldar nossos projetos” (JACOBS, 2014). Para Greenfield (2006), “o espaço público, em todas as suas formas, é uma das poucas ferramentas capazes de servir ao bem comum, portanto, valem os esforços para preservar esse recurso”.

Almeida, Filgueiras e Gaetani (2019) propõem como um dos elementos fundamentais para a governança de serviços públicos digitais a coprodução, promovida pelo diálogo entre os múltiplos atores envolvidos – governo, iniciativa privada, academia e sociedade civil – que assumem um papel ativo na busca de soluções sustentáveis, inclusivas, baseadas em princípios e focadas nas necessidades dos cidadãos.

Governança da Internet refere-se ao "desenvolvimento e aplicação por parte dos governos, do setor privado e da sociedade civil, em seus respectivos papéis, de princípios comuns, normas, regras, procedimentos de tomada de decisão e programas que dão forma à evolução e utilização da Internet” (WEBER, 2013, p. 341). Experiências de regulamentação da Internet sugerem que o conceito de “governança multilateral” pode ser entendido como um caminho a seguir em favor da inclusão da sociedade no processo decisório sobre a IoT. Diferentes mecanismos legais podem ser adotados, tais como: instrumentos jurídicos internacionais que poderiam fundamentar leis nacionais; recomendações direitas das organizações internacionais;

corregulação (mecanismo baseado em objetivos estabelecidos em ato legislativo, mas implementados por particulares); e autorregulação (baseando-se em regras adotadas pela indústria). Parece ser evidente que o ideal é haver uma combinação de vários mecanismos, em uma abordagem de múltiplos níveis (WEBER, 2013).

(IV) Capacidade organizacional e recursos

Este componente trata da capacidade de governança e gestão de organizações, processos e recursos para garantir a implementação da política. De acordo com demonstrado nas seções 5.3.2 e 5.5, foi constatada a articulação dos diversos agentes envolvidos com a política, e identificados uma série de investimentos que vêm sendo realizados para fomento às iniciativas do Plano de IoT, com financiamentos específicos para o setor. E os pilotos demonstraram a exequibilidade dos projetos até o momento. Mas há sempre o risco de descontinuidade das ações, dada a diversidade e complexidade de normativos e programas relacionados à área, somados ao contexto econômico, social e político do país.

Particularmente sobre o crescimento da IoT no Brasil, e reforçando a relevância do tema, no Relatório de Avaliação do PPA, a meta 04IM: “Chegar a 20 milhões de acessos do tipo máquina a máquina” apresentou andamento adequado, alcançando em 2017 o patamar de 18,43 milhões, chegando em 2019 a 22,9 milhões (ANATEL, 2020; MINISTÉRIO DA ECONOMIA, 2018, 2019, 2020).

(V) Coordenação e coerência

Este critério avalia em que medida há coordenação na política, com os diversos sistemas institucionais e gerenciais que a formulam trabalhando juntos; e coerência, que envolve a “promoção sistemática de ações que se reforcem mutuamente nas diferentes partes interessadas, criando sinergias para a realização dos objetivos definidos” (BRASIL, 2014, p. 57). Há um modelo de governança para o Plano de Nacional de IoT descrito na E-digital (2018a) e no estudo do BNDES (2017d), que integra partes interessadas, como cidadãos, iniciativa privada, academia, instituições governamentais e formuladores de políticas, detalhado na seção 5.3.2. É preciso avaliar seu funcionamento na prática, após a implementação das ações do Plano.

O Relatório de Fiscalizações em Políticas e Programas de Governo (RePP), desenvolvido pelo TCU (2019b) em atendimento ao art. 124 da Lei de Diretrizes Orçamentárias (LDO) apresenta como achados:

> Ausência de estrutura atuante de coordenação das políticas federais de fomento à inovação sob uma perspectiva integrada de governo; falhas na Estratégia Nacional de Ciência, Tecnologia e Inovação, como: quantidade excessiva de temas prioritários; ausência de visão de longo prazo para inovação; ausência de planejamento estratégico para o governo como um todo contemplando previsão de acompanhamento da estratégia; falhas na participação de atores relevantes no processo de elaboração; falhas no monitoramento e na avaliação, como: inexistência de histórico de avaliação para parte das políticas, dos programas e das iniciativas; diferentes estágios de maturidade dos processos de monitoramento e avaliação; inexistência de indicadores de resultado e impacto para parte das políticas; e falta de informações para apoiar a realização de monitoramento e avaliação (BRASIL, 2019b).

O Plano Nacional de IoT se enquadra no escopo das políticas de fomento à inovação.

Ronaldo Lemos (2019) defende que uma política de IoT efetiva pressupõe o multisetorialismo, e o Plano Nacional de IoT é insuficiente nesse ponto, ao instituir a Câmara IoT com estrutura interministerial. Segundo o autor, a Câmara IoT deveria ser constituída "de forma permanente por representantes de diversos setores da sociedade, incluindo o setor privado e a comunidade científica. O setor público sozinho pode fazer muito pouco em processos complexos de implementação tecnológica, como é o caso da IoT". De qualquer maneira, apesar da fragilidade da composição original do Decreto (BRASIL, 2019a), a lista de membros foi atualizada pelo MCTIC, conforme Anexo 1, incluindo mais de 60 instituições, dentre órgãos de governo, iniciativa privada, universidades e centros de pesquisa (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 2020b).

(VI) Monitoramento e avaliação

Este componente analisa se o andamento das operações inerentes à política está sendo constantemente monitorado e os seus resultados avaliados, "com vistas à concretização dos objetivos programados e ao aperfeiçoamento do desempenho governamental" (BRASIL, 2014, p. 60). O processo de acompanhamento do Plano está previsto nas atribuições da Câmara IoT e do Observatório Nacional para o Acompanhamento da Transformação Digital (BRASIL, 2019a), detalhados na seção 5.7.

O Observatório busca resolver a questão da dispersão de informações, apresentando-se como ponto centralizado de políticas públicas sobre o tema. Entretanto, as informações apresentadas sobre o acompanhamento das ações são insuficientes e desatualizadas em termos de indicadores, metas e desempenho físico-

financeiro. Ademais, não houve retorno à tentativa de contato pelo portal do Observatório, conforme relatado, prejudicando a transparência da política. Isso sugere que a estrutura concebida para o monitoramento da política pode não estar em efetivo funcionamento.

(VII) Gestão de riscos e controle interno

Este componente trata da gestão de riscos, definida como “atividades coordenadas para dirigir e controlar uma política no que se refere aos riscos” (BRASIL, 2014, p. 63). O plano de ação (BNDES, 2017) prevê estrutura de monitoramento que deve mapear o status e os possíveis riscos do andamento das iniciativas. A compatibilização do arcabouço normativo relacionado à diversidade de aplicações da IoT é um risco mapeado. Precisa ocorrer de forma efetiva para que as soluções contemplem seus múltiplos aspectos e interesses, conforme detalhado na seção 5.4. A gestão efetiva dos riscos dependerá essencialmente do funcionamento da estrutura de monitoramento abordada no item VII.

(VIII) Accountability

Este critério envolve os aspectos relacionados à “transparência, responsabilização, comunicação e prestação sistemática de contas” (BRASIL, 2014, p. 65). Uma crítica geral à política é a dificuldade em relacionar a documentação pertinente, e criar um mapa das iniciativas e regulamentações antecedentes e vigentes das políticas e planos relacionados e do andamento das ações. Há muito material de qualidade disponível nos sites governamentais e privados sobre o tema, mas é preciso melhorar a transparência e a centralização de dados dos veículos públicos, especialmente em tempos de descontinuidade de iniciativas, mudança de governo e revisão de prioridades.

A seção 5.1.4 indica algumas das políticas relacionadas com o Plano Nacional de IoT, mas a sistematização desse histórico e dessas relações não é trivial. Um exemplo é o Plano Nacional de Conectividade (PNC), que teria relação direta com a política de IoT. A última notícia encontrada sobre o PNC é de 2017, após a abertura da consulta pública. Não há informações claras sobre o que aconteceu com o Plano.

7. Considerações finais

O objetivo deste trabalho foi realizar análise *ex ante* do Plano Nacional de Internet das Coisas (IoT) e de seus impactos para o desenvolvimento das cidades inteligentes no Brasil, com enfoque nas questões relacionadas à privacidade e proteção de dados dos cidadãos, no escopo das soluções de mobilidade urbana, segurança pública e eficiência energética propostas nos projetos-piloto da política.

No diagnóstico foram apresentados dados sobre as causas e evidências de problemas urbanos como congestionamentos, violência nas cidades e consumo de energia elétrica no Brasil, e as propostas de soluções com o uso de tecnologias de IoT. Alguns casos internacionais de políticas similares foram ilustrados, bem como as razões para intervenção do Estado e as políticas relacionadas, em andamento ou finalizadas.

Posteriormente, as propostas foram analisadas sob a ótica da privacidade e proteção de dados dos cidadãos. O modelo lógico apresentou um resumo dos problemas, beneficiários, executores, insumos, atividades, produtos e resultados relacionados aos projetos-piloto financiados pelo BNDES, selecionados para análise neste trabalho. Outras iniciativas de fomento governamental federal para IoT foram identificadas e brevemente resumidas na seção sobre impacto orçamentário e financeiro.

Foi realizado ainda um mapeamento dos principais atores envolvidos com a política, e descrito o modelo de governança proposto pelo estudo que subsidiou a elaboração do Plano, com algumas evidências de seu funcionamento na prática. Há indícios de que houve engajamento de diversos atores na elaboração do plano de ação para IoT, num processo de construção colaborativa demonstrado pelos relatórios, entrevistas, consultas públicas e eventos, que se constituem em mecanismos eficientes de confiança e suporte da política.

Nos aspectos legislativos e regulatórios, o trabalho explorou a relação da Lei Geral de Proteção de Dados Pessoais e do Marco Civil da Internet e seus impactos para as aplicações de IoT em termos de privacidade em cidades inteligentes. Analisou também, de forma subsidiária e não-exaustiva, outros normativos que compõem o quadro legal relacionado ao tema, como a Estratégia de Governo Digital, a Política Nacional de Segurança da Informação, o Cadastro Base do Cidadão e o Comitê

Central de Governança de Dados. Identificou ainda iniciativas da Anatel para garantir a conformidade das soluções com padrões e normas, conforme descrito na análise de impacto regulatório realizada pela agência.

Por fim, a análise crítica abordou os oito elementos do modelo de governança de políticas públicas do Referencial do TCU (2014). Em resumo, concluiu que:

a. A política está institucionalizada em instrumentos formais;
b. há coesão entre planos e objetivos, mas existem questões relativas à privacidade que precisam ser equacionadas, como o funcionamento efetivo da já instituída Autoridade Nacional de Proteção de Dados, para garantir a aplicação da LGPD e de normas correlatas, assegurando, entre outras questões, a observância a princípios como legalidade, finalidade e proporcionalidade no tratamento e compartilhamento de dados pessoais sensíveis no âmbito das soluções de IoT;
c. há representatividade dos diversos atores do ecossistema de IoT no desenho e implementação da política, mas a participação efetiva desses agentes nos fóruns, garantindo o multisetorialismo, precisa ser uma busca constante em prol da defesa do interesse público nas definições e intervenções da política;
d. há uma percepção sobre a falta de coordenação do governo federal acerca das ações de inovação, relatada no RePP (2019b), que gera eventual dispersão de informações e recursos, causando dificuldades de compreensão das iniciativas de fomento pelos atores e da captação de incentivos;
e. no desenho e implementação dos projetos-piloto selecionados, ficaram claros o público-alvo e os critérios de priorização e seleção de beneficiários, a execução orçamentária e financeira dos referidos projetos, em princípio, tem ocorrido da forma planejada;
f. há mais de uma política que tangencia o tema IoT, e a correlação entre as iniciativas e sua continuidade não são evidentes, especialmente as que se iniciaram antes do governo atual;
g. há espaços para aperfeiçoamento da compatibilidade de realidades entre os diferentes municípios beneficiários das políticas, tanto do ponto de vista de infraestrutura e recursos, quanto de compatibilidade normativa no

arcabouço legal local que circunda as inciativas, particularmente nas áreas analisadas, de mobilidade urbana, segurança pública e eficiência energética. Uma política com enfoque nas cidades, que se proponha a sistematizar soluções adequadas à realidade de cada município ou região, e ao mesmo tempo busque alinhamento conceitual em termos de diretrizes e boas práticas para o alcance de níveis de maturidade de desenvolvimento em cidades inteligentes talvez seja um caminho. Foram identificadas propostas nessa linha, como a Política Nacional para Cidades Inteligentes e seus desdobramentos; e

h. há lacunas em relação à transparência das ações, com informações dispersas e desatualizadas nos veículos oficiais, apesar da consistência do modelo de monitoramento e avaliação proposto para a política e da existência de mecanismos para o controle, como a Câmara IoT e o Observatório da Transformação Digital.

O Guia Prático de Análise *Ex Ante* de Políticas Públicas (2018) demonstrou ser uma metodologia adequada aos objetivos deste trabalho, pois possibilitou a sistematização de informações relevantes relativas à política em um encadeamento lógico sob a perspectiva *ex ante*. Da mesma forma, a partir do Referencial para Avaliação da Governança de Políticas Públicas do TCU (2014) foi possível evidenciar aspectos-chave que permitiram uma análise qualitativa da política em questão.

É preciso considerar que a política trata dos chamados *wicked problems*, na medida em que se enquadram em quase todas as categorias apresentadas por Guy Peters (2015), que aplica o conceito aos problemas de políticas públicas: a) sem clara delimitação de fronteiras, com convergência de soluções públicas e privadas, e multiplicidade de atores envolvidos, além de potenciais conflitos, com maior necessidade de coordenação; b) relacionados a bens públicos, que justificam a intervenção do Estado; c) que envolvem escala e múltiplas soluções, que precisam ser desenvolvidas em conjunto; d) difíceis de resolver, ou que criam novos problemas; e) complexos do ponto de vista técnico ou político; f) que envolvem incerteza e risco, ou situações que não podem ser previstas; e g) caracterizados por “escolhas trágicas”, que envolvem decisões que geram benefícios ao mesmo tempo em que impõem perdas (ex: privacidade x segurança).

Pela definição, originalmente proposta por Horst Rittel (1972), *wicked problems* são problemas sociais ou culturais únicos, de difícil solução, ou que não podem ser solucionados, apenas mitigados, por envolverem: conhecimento incompleto ou contraditório, grande número de pessoas e opiniões, ônus econômico e natureza interconectada com outros problemas.

Chen (2020) classifica os problemas de cidades inteligentes como *wicked* e faz as seguintes recomendações de como trata-los: reconhecê-los como *wicked* e buscar soluções apropriadas; pensar de forma sistêmica, considerando as correlações entre os fatores; buscar colaboração constante com os múltiplos atores, envolvendo decisores e cidadãos; e aceitar a falha como parte do processo de solução. Buchanan (1992) propõe uma abordagem de *design thinking* para a busca de soluções colaborativas para os *wicked problems*, que enfatiza a empatia, o raciocínio abdutivo e a prototipagem rápida.

O estudo que subsidiou a elaboração do Plano de IoT demonstra, em sua magnitude, a complexidade e infinidade de fatores que envolvem a política, na tentativa de prever os impactos e basear em evidências as decisões sobre o desenho e a implementação da política.

As tecnologias são capazes de ampliar o potencial de gestão e oferta de serviços públicos em uma cidade inteligente, promovendo a melhoria da qualidade de vida dos cidadãos. Os benefícios são inegáveis. Mas a instrumentação tecnológica por si só não garante o alcance do interesse público. As soluções devem ser essencialmente focadas nas necessidades dos cidadãos, ou seja, na criação de experiências significativas para as pessoas, a partir de premissas como transparência e preservação de direitos fundamentais.

Na busca do equilíbrio entre valores contraditórios como segurança pública e privacidade, por exemplo, é preciso investigar de forma sistêmica as causas da violência urbana. E essa resposta encontra uma variedade de fatores, que envolve outras políticas públicas, como educação, saúde, saneamento e garantia de mínimas condições de vida. As soluções não são óbvias e não se resolvem com perspectivas simplistas.

Os casos das cidades colombianas de Bogotá e Medellín, em suas políticas de enfrentamento à criminalidade, são emblemáticos. O documentário “E^2 design: Bogotá: building a sustainable city” (2007) mostra a transformação de uma das cidades mais caóticas do mundo em um modelo de planejamento urbano sustentável.

Ao invés de apenas armas e mais policiais, foram priorizadas a construção de escolas, bibliotecas e equipamentos públicos de qualidade, a reforma de praças, a urbanização de áreas periféricas, com vias exclusivas para bicicletas e pedestres, além de transporte público acessível a todos. Os índices de homicídios caíram de 80 por 100 mil habitantes em 1993 para 22 em 2011. Em Medellín, a taxa que chegava a 360 homicídios a cada 100 mil habitantes, caiu para 20, quase 90% de redução (CARVALHO, 2019).

Essa visão é semelhante a uma das interpretações da "teoria das janelas quebradas", que considera não o aumento de policiamento, mas "a limpeza de terrenos baldios e outras práticas de solução de problemas com base em lugares [*placemaking*] para reduzir a desordem social", eliminando a sensação de abandono e descaso (FOX, 2019).

Ao lidar com problemas complexos, a reação das pessoas às intervenções pode gerar comportamentos inesperados, que não foram previstos pelo designer no momento de projetar a solução. Por isso, a recomendação é de projetar para gerar influências (*nudges*), não controle. Para Sunstein (2014), *nudges* constituem intervenções que preservam a liberdade de escolha, ainda que possam influenciar a tomada de decisão. A premissa é induzir, não coagir.

O recente caso do combate à Covid-19 ilustra bem esse princípio. Os países têm se valido da tecnologia com abordagens baseadas em diferentes princípios para solucionar o problema. Na China, foi adotado um sistema de vigilância tecnológica via celular, pelo qual as autoridades atribuem ao dono do aparelho um código de barras e uma cor, em função do risco de estar com a doença, e enviam os dados à polícia. A solução não apresenta transparência e nem garante privacidade. A Coreia do Sul, por sua vez, usa localização dos celulares, imagens de câmeras e dados de cartão de crédito para reconstituir a trajetória dos portadores do coronavírus. Cingapura adotou um modelo menos invasivo, via *bluetooth*, pelo qual o cidadão baixa um aplicativo do governo e passa a registrar os celulares que passam perto. O sistema, então, avisa aos que cruzaram com pessoas contaminadas, mas mantém a privacidade de ambos. Pesquisadores do Instituto de Tecnologia de Massachussetts (MIT) publicaram um estudo (RASKAR et al., 2020) com premissas para o desenvolvimento de um sistema similar, que é justamente baseado em indução de comportamentos (*nudges*), não em coação. O uso do aplicativo por 10% da população seria suficiente para reduzir a velocidade de contágio (GUROVITZ, 2020).

A implantação de internet das coisas em cidades inteligentes requer uma abordagem humanista e sistêmica, baseada essencialmente em princípios, com vistas a evitar soluções pautadas em valores exclusivamente comerciais ou tecnicistas (LACERDA; LIMA-MARQUES, 2015). Princípios compartilhados, como transparência, responsabilidade, justiça e responsividade, promovem a oferta de serviços públicos digitais inclusivos, eficazes e legítimos, aderentes às expectativas e necessidades dos cidadãos (ALMEIDA; FILGUEIRAS; GAETANI, 2019).

Este trabalho abordou apenas as ações a cargo do Estado. Iniciativas de implementação de soluções de IoT em espaço público pela iniciativa privada não foram diretamente tratadas no escopo da discussão, mas devem se guiar pelos mesmos princípios, na medida que intervenções no espaço público devem ser necessariamente reguladas. Nesse sentido, Evgeny Morozov (2020) traz o conceito de soberania tecnológica como "pré-requisito para que as cidades possam conduzir políticas públicas autônomas e independentes". Segundo o autor, "muitas cidades estão basicamente assinando contratos com as empresas de tecnologia que não apenas colocam os dados dos cidadãos em uma situação potencialmente comprometedora, mas também fazem com que seja quase impossível criar políticas públicas autônomas".

> As novas tecnologias de informação e comunicação das chamadas 'smart cities' precisam tornar-se parte indissociável das políticas públicas urbanas, em um esforço concertado para construção de uma agenda positiva […] não é possível alcançar resultados significativos de redução da violência urbana se os investimentos em novas tecnologias de monitoramento não estiverem articulados a esforços que visem à redução da pobreza, das desigualdades socioespaciais, da falta de moradia adequada ou à ampliação das oportunidades de trabalho, das estruturas de educação e cultura, etc. (FERRAZ, 2017).

O Plano Nacional de IoT parte da perspectiva da instrumentação da cidade pela inserção de sensores e atuadores nos objetos que compõem a estrutura urbana, como postes, veículos, lixeiras, etc. Entretanto, do ponto de vista fenomenológico (LACERDA; LIMA-MARQUES; RESMINI, 2019), é preciso considerar a cidade em toda sua complexidade, tendo como foco o sujeito, a experiência do cidadão.

> Pactuar uma visão comum sobre cidades inteligentes no contexto brasileiro é crucial para o futuro de nossas cidades e para a articulação de políticas, programas, iniciativas e investimentos públicos que permitam às cidades navegarem neste mundo em transformação protegendo as parcelas mais vulneráveis da população (WRI BRASIL, 2020).

De qualquer forma, o Plano Nacional de IoT é o primeiro passo para a implementação de cidades inteligentes no Brasil. Seu desenho parece ser efetivo para o alcance dos objetivos de curto prazo, como demonstrado na execução dos Pilotos IoT do BNDES. A longo prazo, é preciso que haja maior articulação entre as diversas políticas, iniciativas e linhas de fomento, para que os esforços não sejam dispersos, sejam consideradas as diferenças regionais e seja instituída uma política com visão holística sobre os problemas da cidade.

É necessário ainda o buscar o equilíbrio constante entre soluções que considerem o interesse público por princípio, sem criar barreiras que inviabilizem as inovações. A expectativa é de que o Programa Brasileiro para Cidades Inteligentes Sustentáveis, como parte da Política Nacional para Cidades Inteligentes, traga uma perspectiva mais sistêmica, o que não invalida as ações implementadas no escopo do Plano.

Referências bibliográficas

AGÊNCIA BRASIL. **Atualização do PNBL deverá ter recursos apenas em 2019, diz presidente da Anatel**. Disponível em: https://agencia-brasil.jusbrasil.com.br/noticias/464554588/atualizacao-do-pnbl-devera-ter-recursos-apenas-em-2019-diz-presidente-da-anatel. Acesso em: 16 jun. 2020.

AGÊNCIA BRASIL. **Regulamentação de nova lei de telecomunicações deve levar um ano**. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2019-10/regulamentacao-de-nova-lei-de-telecomunicacoes-deve-levar-um-ano. Acesso em: 16 jun. 2020.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Informe nº 146/2018/SEI/PRRE/SPR**. Brasília: Anatel, 2018. Disponível em: https://cutt.ly/Cy42aWq. Acesso em: 4 fev. 2020.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Análise Nº 84/2019/MM**. Brasília: Anatel, 2019. Disponível em: https://cutt.ly/zy42WL9. Acesso em: 4 fev. 2020.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Acessos de telefonia móvel no Brasil**. [s.l: s.n.]. Disponível em: https://www.anatel.gov.br/dados/destaque-1/283-movel-acessos-maio. Acesso em: 1 jul. 2020.

ALMEIDA, V.; FILGUEIRAS, F.; GAETANI, F. Principles and Elements of Governance of Digital Public Services. **IEEE Internet Computing**, v. 23, n. 6, p. 48–53, dez. 2019.

ASSOCIAÇÃO BRASILEIRA DE INTERNET DAS COISAS (ABINC). **Políticas para IoT**. Disponível em: https://abinc.org.br/politicas-para-iot/. Acesso em: 12 fev. 2020.

BABUTA, A.; OSWALD, M. Data Analytics and Algorithmic Bias in Policing. **Royal United Services Institute for Defence and Security Studies**, 16 set. 2019.

BNDES. **Relatório de aprofundamento das verticais: cidades**: Internet das Coisas: um plano de ação para o Brasil. São Paulo: McKinsey & Company, 2017a. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/776017fa-7c4a-43db-908f-c054639f1b88/relatorio-aprofundamento+das+verticais-cidades-produto-7A.pdf?MOD=AJPERES&CVID=m3rPg5Q. Acesso em: 11 jun. 2020.

BNDES. **Relatório do plano de ação: capítulo regulatório**: Internet das Coisas: um plano de ação para o Brasil. São Paulo: McKinsey & Company, 2017b. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/f9582d36-4355-4638-b931-e2e53af5e456/8B-relatorio-final-plano-de-acao-produto-ambiente-regulatorio.pdf?MOD=AJPERES&CVID=m7tyLs1. Acesso em: 11 jun. 2020.

BNDES. **Benchmark de iniciativas e políticas públicas**. Brasília: BNDES, abr. 2017c. Disponível em: https://cutt.ly/ly42A4D. Acesso em: 11 jun. 2020.

BNDES. **Internet das Coisas: um plano de ação para o Brasil**. São Paulo: McKinsey & Company, nov. 2017d. Disponível em: http://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil. Acesso em: 13 fev. 2020.

BNDES. **BNDES Pilotos IoT: Internet das Coisas**. Disponível em: http://www.bndes.gov.br/wps/portal/site/home/onde-atuamos/inovacao/internet-das-coisas/bndes-projetos-piloto-internet-das-coisas. Acesso em: 5 jun. 2020.

BNDES. **Cartilha de Cidades**. São Paulo: McKinsey & Company, 2018b. Disponível em: http://www.bndes.gov.br/wps/portal/site/home/transparencia/consulta-operacoes-bndes. Acesso em: 11 jun. 2020.

BNDES. **Chamada Pública para Seleção de Fundo de Investimento em Participações em Internet das Coisas - Internet of Things (IoT)**. Disponível em: h https://www.bndes.gov.br/wps/wcm/connect/site/db27849e-dd37-4fbd-9046-6fda14b53ad0/produto-13-cartilha-das-cidades-publicada.pdf?MOD=AJPERES&CVID=m7tz8bf. Acesso em: 18 jun. 2020.

BNDES. **Consulta a operações do BNDES**. Brasília: BNDES, 2020. Disponível em: http://www.bndes.gov.br/wps/portal/site/home/transparencia/consulta-operacoes-bndes. Acesso em: 11 jun. 2020.

BRASIL. **Lei nº 9.472, de 16 de julho de 1997**, 16 jul. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9472.htm. Acesso em: 26 fev. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014** - Marco Civil da Internet. . 23 abr. 2014.

BRASIL. **Lei nº 13.249, de 13 de janeiro de 2016**, jan. 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Lei/L13249.htm. Acesso em: 13 fev. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**, 14 ago. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 fev. 2020.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**, 26 dez. 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 1 jun. 2020.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**, 25 jun. 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. Acesso em: 13 fev. 2020.

BRASIL. **Lei nº 13.853, de 08 de julho de 2019**, 8 jul. 2019b. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:federal:lei:2019-07-08;13853. Acesso em: 27 jun. 2020.

BRASIL. **Lei nº 13.879, de 03 de outubro de 2019**, 4 out. 2019c. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:federal:lei:2019-10-03;13879. Acesso em: 4

fev. 2020.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**, 9 out. 2019d. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 27 jun. 2020.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**, 5 fev. 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 1 jun. 2020.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**, 28 abr. 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10332.htm#art12. Acesso em: 27 jun. 2020.

BRASIL. **Medida Provisória nº 959/2020**, 29 abr. 2020c. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:congresso.nacional:medida.provisoria;mpv:2020-04-29;959. Acesso em: 28 jun. 2020.

BRASIL. **Lei nº 14.000, de 19 de maio de 2020**, 19 maio 2020d. Disponível em: http://www.in.gov.br/en/web/dou/-/lei-n-14.000-de-19-de-maio-de-2020-257608960. Acesso em: 17 jun. 2020.

BRASIL. **Lei nº 14.010 de 10 de junho de 2020**, 10 jun. 2020e. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:federal:lei:2020-06-10;14010. Acesso em: 27 jun. 2020.

BRASIL. Casa Civil da Presidência da República. **Portal da Legislação do Planalto**. Disponível em: http://www4.planalto.gov.br/legislacao/copy_of_home. Acesso em: 27jun. 2020.

BRASIL. Casa Civil da Presidência da República; Instituto de Pesquisa Econômica Aplicada. **Avaliação de políticas públicas: guia prático de análise ex ante**. Brasília: Ipea, 2018. v. 1. Disponível em: https://www.cgu.gov.br/Publicacoes/auditoria-e-fiscalizacao/arquivos/guia-analise-ex-ante.pdf. Acesso em: 11 fev. 2020.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. **Estratégia Brasileira para a Transformação Digital: E-digital**. Brasília: MCTIC, 2018a. Disponível em: http://www.mctic.gov.br/estrategiadigital. Acesso em: 19 jun. 2020.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. **Portaria nº 5.894, de 13 de novembro de 2018**, 13 nov. 2018b. Disponível em: http://www.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCTIC_n_5894_de_13112018.html?searchRef=deter&tipoBusca=expressaoExata. Acesso em: 19 jun. 2020.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. **Portaria nº 1.122, de 19 de março de 2020**, 19 mar. 2020. Disponível em:http://www.in.gov.br/en/web/dou/-/portaria-n-1.122-de-19-de-marco-de-2020- 249437397. Acesso em: 3 jul. 2020.

BRASIL. Tribunal de Contas da União. **Referencial para avaliação de governança em políticas públicas**. Brasília: TCU, 2014.

BRASIL. Tribunal de Contas da União. **Acórdão 1898/2017 - Plenário. Bruno Dantas**, 30 ago. 2017. Disponível em: shorturl.at/txT13. Acesso em: 5 jul. 2020.

BRASIL. Tribunal de Contas da União. **Relação das Situações Problemas da SeinfraCom**, 2019a.

BRASIL. Tribunal de Contas da União. **Relatório de Políticas e Programas de Governo (RePP): 2019**. Brasília: TCU, 2019b. Disponível em: https://portal.tcu.gov.br/relatorio-de-politicas-e-programas-de-governo-repp.htm. Acesso em: 2 jul. 2020.

BRASIL. Tribunal de Contas da União. **Acórdão 1613/2020 - Plenário. Aroldo Cedraz**, 24 jun. 2020. Disponível em: shorturl.at/ertB9. Acesso em: 3 jul. 2020.

BURGESS, M. Facial recognition tech used by UK police is making a ton of mistakes. **Wired UK**, 4 maio 2018.

CARVALHO, I. **Medellín: da cidade mais violenta para a mais inovadora do mundoStartSe**, 15 fev. 2019. Disponível em: https://www.startse.com/noticia/ecossistema/medellin-da-cidade-mais-violenta-para-a-mais-inovadora-do-mundo. Acesso em: 4 jul. 2020.

CENTRO DE PESQUISAS E DESENVOLVIMENTO EM TELECOMUNICAÇÕES (CPQD). **Projeto do CPQD de pilotos IoT para cidades inteligentes é aprovado pelo BNDESCPQD**, 26 nov. 2019. Disponível em: https://www.cpqd.com.br/releases/projeto-do-cpqd-de-pilotos-iot-para-cidades-inteligentes-e-aprovado-pelo-bndes/. Acesso em: 11 jun. 2020.

CHEN, C. Y. **Smart cities: a tamable wicked problem for the 21st centuryEnergy Central**, 2020. Disponível em: https://energycentral.com/c/iu/smart-cities-tamable-wicked-problem-21st-century. Acesso em: 23 jun. 2020.

COALITION FOR CRITICAL TECHNOLOGY. **Abolish the #TechToPrisonPipeline**. Disponível em: https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16. Acesso em: 25 jun. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS. Instrução CVM 578. 30 ago. 2016. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst578.html. Acesso em: 28 jun. 2020.

DEPINÉ, Á. et al. Cidade inteligente: a transformação do espaço urbano pela tecnologia. In: DEPINÉ, Á.; TEIXEIRA, C. S. (Eds.). **Habitats de inovação: conceito e prática**. São Paulo: Perse, 2018. v. 1p. 32–66.

DW BRASIL. **O dilema europeu da vigilância pública em detrimento da privacidade**, 7 nov. 2017. Disponível em: https://www.youtube.com/watch?time_continue=175&v=cDc633326qM&feature=emb_logo. Acesso em: 28 jun. 2020.

E^2 design: Bogotá: Building a sustainable city. , 14 dez. 2007. Disponível em: https://www.pbs.org/e2/episodes/209_bogota_building_sustainable_city_trailer.html.

Acesso em: 4 jul. 2020.

EFUS. **Citizens, Cities and Video Surveillance**European Forum for Urban Security, 31 maio 2010. Disponível em: https://issuu.com/efus/docs/cctv_charter_pt. Acesso em: 1 jul. 2020.

EFUS. **Manifesto: Segurança, Democracia e Cidades: coproduzir as políticas de segurança** Fórum Europeu para a Segurança Urbana, , 29 abr. 2018. Disponível em:https://issuu.com/efus/docs/manifeste-vpt-web. Acesso em: 1 jul. 2020.

EMBRAPII. **EMBRAPII contará com R$ 8 milhões para investir em IoT e Manufatura 4.0**. Disponível em: https://embrapii.org.br/embrapii-contara-com-r-8-milhoes-para-investir-em-iot-e-manufatura-4-0/. Acesso em: 24 jun. 2020.

EUROPEAN COMMISSION. **Conclusions of the Internet of Things public consultation**. Brussels: [s.n.]. Disponível em: ec.europa.eu//digital-agenda/en/news/conclusions-internet-things-public-consultation. Acesso em: 1 jan. 2015.

EUROPEAN UNION. **Data Protection Impact Assessment (DPIA)**. Disponível em: https://gdpr.eu/data-protection-impact-assessment-template/. Acesso em: 1 jul. 2020.

FERRAZ, F. As cidades inteligentes devem ser reflexo de uma sociedade inteligente. **Nexo**, ago. 2017. Disponível em: shorturl.at/ozZ06. Acesso em: 24 jun. 2020.

FINEP. **Finep IoT**. Disponível em: http://www.finep.gov.br/apoio-e-financiamento-externa/programas-e-linhas/finep-iot. Acesso em: 24 jun. 2020.

FOUCAULT, M. **Vigiar e Punir**. Lisboa: Leya, 2014.

FOX, J. A “Teoria das Janelas Quebradas” estava certa... sobre as janelas. **Gazeta do Povo**, 30 out. 2019.

FRAGOSO, N.; MASSARO, H. Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina? **Jota: Opinião e Análise**, 19 dez. 2019.

FUNDACIÓN BANKINTER INNOVACIÓN. **The Internet of things**. Madrid: FBI, 2011. Disponível em: http://www.fundacionbankinter.org/en/publications/the-internet-of-things. Acesso em: 24 ago. 2014.

GOMYDE, A. Cidades inteligentes e humanas. **Boletim de Conjuntura do Setor Energético**, FGV Energia. fev. 2017.

GONÇALVES, F.; GONÇALVES, G. 94% dos brasileiros reconhecem que pessoas negras têm mais chances de serem abordadas de forma violenta e mortas pela polícia, diz pesquisa. **G1**, 17 jun. 2020.

GREENFIELD, A. **Everyware: The Dawning Age of Ubiquitous Computing**. San Francisco: New Riders Publishing, 2006.

GREENFIELD, A. **Public Objects and the Connected City**. In: DRCR. Bristol, maio 2010. Disponível em: http://www.dcrc.org.uk/2011/05/10/public-objects-and-connected-city-adam-greenfields-talk/. Acesso em: 11 jan. 2015.

GREENFIELD, A.; KIM, N. **Against the smart city: the city is here for you to use**. [s.l.] Do projects, 2013.

GRIERSON, J. Predictive policing poses discrimination risk, thinktank warns. **The Guardian**, 15 set. 2019.

GROSSMANN, L. O. Anatel abre consulta pública para incentivar o fomento da Internet das Coisas. **Abranet: Associação Brasileira de Internet**, 11 set. 2018.

GUROVITZ, H. É possível rastrear sem invadir. **G1**, 13 abr. 2020.

HUSTINX, P. Privacy by design: delivering the promises. **Identity in the Information Society**, v. 3, n. 2, p. 253–255, 1 ago. 2010.

IBGE. **Censo demográfico 1940-2010**: Séries Estatísticas & Séries Históricas. Rio de Janeiro: IBGE, 2007. Disponível em: https://seriesestatisticas.ibge.gov.br/series.aspx?vcodigo=POP122. Acesso em: 13 fev. 2020.

IDC. The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. **IDC: The premier global market intelligence company**, 18 jun. 2019.

IDEC. **Justiça impede uso de câmera que coleta dados faciais em metrô em SP**. Disponível em: https://idec.org.br/noticia/justica-impede-uso-de-camera-que-coleta-dados-faciais-do-metro-em-sp. Acesso em: 3 jun. 2020.

IERC. **European Research Cluster on the Internet of Things**. Disponível em: http://www.internet-of-things-research.eu/. Acesso em: 3 set. 2013.

JACOBS, J. **Morte e vida de grandes cidades**. São Paulo: Martins Fontes, 2014.

KNOPIK, M. J. V. Políticas públicas e a Internet das Coisas: sugestões para a operacionalização jurídica das cidades hiper conectadas. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, v. 3, n. 3, dez. 2018.

KOCH, R. **LGPD: a versão brasileira do regulamento europeuSerpro**, 12 set. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais. Acesso em: 26 jun. 2020.

KUNIAVSKY, M. **Smart Things: Ubiquitous Computing User Experience Design**. Amsterdam: Elsevier, 2010.

LACERDA, F. **Arquitetura da Informação Pervasiva: projetos de ecossistemas de informação na internet das coisas**. Tese de Doutorado—Brasília: Universidade de Brasília, 2 dez. 2015. Disponível em: https://repositorio.unb.br/bitstream/10482/19646/1/2015_FlaviaLacerda.pdf. Acesso em: 30 jun. 2015.

LACERDA, F.; LIMA-MARQUES, M. Da necessidade de princípios de Arquitetura da Informação para a Internet das Coisas. **Perspectivas em Ciência da Informação**, v. 20, n. 2, p. 158–171, 30 jun. 2015.

LACERDA, F.; LIMA-MARQUES, M.; RESMINI, A. An Information Architecture Framework for the Internet of Things. **Philosophy & Technology**, v. 32, n. 4, p. 727–744, 1 dez. 2019. Disponível em: https://link.springer.com/article/10.1007/s13347-018-0332-4. Acesso em: 30 jun. 2020.

LEMOS, R. Aprovado o plano de internet das coisas: Brasil é exímio elaborador de planos, mas ainda não os conseguimos executar. **Folha de São Paulo**, 3 jul. 2019.

LOWI, T. J. Four Systems of Policy, Politics, and Choice. **Public Administration Review**, v. 32, n. 4, p. 298–310, 1972.

LUCAS, P.; BALLAY, J.; MCMANUS, M. **Trillions: Thriving in the Emerging Information Ecology**. Hoboken, N.J: Wiley, 2012.

MCEWEN, A.; CASSIMALLY, H. **Designing the Internet of Things**. Chichester: Wiley, 2013.

MENDES, G. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695Min. Gilmar Mendes**, 24 jun. 2020. Disponível em: https://www.stf.jus.br/portal/autenticacao/autenticarDocumento.asp?. Acesso em: 27 jun. 2020.

MENDES, P. **Social-driven internet of connected objects**. Proc. of the Interconn. Smart Objects with the Internet Workshop. **Anais**...Citeseer, 2011.Disponível em: https://www.iab.org/wp-content/IAB-uploads/2011/03/Mendes.pdf. Acesso em: 27 jun. 2020.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. **MCTIC vai padronizar Cidades Inteligentes e debater soluções**. Disponível em: http://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2019/07/MCTIC_vai_padronizar_Cidades_Inteligentes_e_debater_solucoes.html. Acesso em: 7 jun. 2020.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. **Inovação: Internet das Coisas**. Disponível em: https://www.mctic.gov.br/mctic/opencms/inovacao/paginas/politicasDigitais/internet_coisas/index.html. Acesso em: 30 jun. 2020a.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. **Câmara IoT**. Disponível em: shorturl.at/ghLUW. Acesso em: 30 jun. 2020b.

MINISTÉRIO DA ECONOMIA. **PPA 2016-2019: relatório anual de avaliação: ano-base 2017**. Disponível em: shorturl.at/vCHY3. Acesso em: 2 jul. 2020.

MINISTÉRIO DA ECONOMIA. **PPA 2016-2019: relatório anual de avaliação: ano-base 2018**. Disponível em: shorturl.at/cjszA. Acesso em: 2 jul. 2020.

MINISTÉRIO DA ECONOMIA. **PPA 2016-2019: relatório anual de avaliação: ano-base 2019**. Disponível em: shorturl.at/agQ14. Acesso em: 2 jul. 2020.

MITCHELL, W. J. **City of Bits: Space, Place, and the Infoban**. Cambridge: MIT Press, 1996.

MOROZOV, E. **Cidades inteligentes não passam de conto de fadas**, 26 mar. 2020. Disponível em: https://tab.uol.com.br/noticias/redacao/2020/03/26/cidades-inteligentes-nao-passam-de-conto-de-fadas-provoca-evgeny-morozov.htm. Acesso em: 5 jun. 2020.

NEWCOMBE, T. **Santander: The Smartest Smart City**. Disponível em: https://www.governing.com/topics/urban/gov-santander-spain-smart-city.html. Acesso em: 1 jul. 2020.

OBSERVATÓRIO DA TRANSFORMAÇÃO DIGITAL. **Internet das Coisas e o Plano Nacional de IoT**. Disponível em: http://otd.cpqd.com.br/otd/index.php/plano-nacional-de-iot/. Acesso em: 19 fev. 2020a.

OBSERVATÓRIO DA TRANSFORMAÇÃO DIGITAL. **Ações do plano nacional de IoT**, 2018b. Disponível em: http://otd.cpqd.com.br/otd/index.php/acoes-do-plano-nacional-de-iot/. Acesso em: 6 jun. 2020.

OLIVEIRA, A.; CAMPOLARGO, M. **From Smart Cities to Human Smart Cities**. 2015 48th Hawaii International Conference on System Sciences (HICSS). **Anais**...dez. 2014. Disponível em: shorturl.at/lXZ27. Acesso em: 25 fev. 2020.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Revisão do Governo Digital no Brasil: rumo à tranformação digital do setor público**: Projeto Governo Digital OCDE. Paris: OCDE, 2018. Disponível em: https://www.slideshare.net/colaborativismo/reviso-do-governo-digital-no-brasil. Acesso em: 19 fev. 2020.

PETERS, B. G. **Advanced Introduction to Public Policy**. Cheltenham, UK ; Northampton, MA: Edward Elgar Publishing, 2015.

POLLO, L. **Cidade-berço do MIT bane reconhecimento facial; decisão tem peso simbólicoTAB: Tendência e Inovação**, 16 jan. 2020. Disponível em: https://tab.uol.com.br/noticias/redacao/2020/01/16/cambridge-bane-reconhecimento-facial-entenda-por-que-temos-de-pensar-nisso.htm. Acesso em: 25 jun. 2020.

PORTER, M. E.; HEPPELMANN, J. E. How Smart, Connected Products Are Transforming Companies. **Harvard Business Review**, dez. 2015.

PROCOPIUCK, M. **Políticas públicas e fundamentos da administração pública: análise e avaliação, governança e redes de políticas, administração judiciária**. São Paulo: Editora Atlas, 2013.

RASKAR, R. et al. Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. **Whitepaper: Private Kit MIT**, p. 15, 19 mar. 2020.

RITTEL, H. On the Planning Crisis : Systems Analysis of the “First and Second Generations”. **Bedriftskonomen**, v. 8, p. 390–396, 1972.

SAMUELSON, P. Self-plagiarism or fair use. **Communications of the ACM**, v. 37, n. 8, p. 21–25, 1 ago. 1994.

SANTUCCI, G. **On the Philosophy of the Internet of Things**. . In: INTERNET OF THINGS PHILOSOPHY. York St John University: 3 jul. 2014. Disponível em: shorturl.at/tyC13. Acesso em: 1 fev. 2015.

SEGURIDAD, JUSTICIA Y PAZ. **Boletín Ranking 2019 de las 50 ciudades más violentas del mundo**. Mexico. Disponível em: shorturl.at/tMSZ7. Acesso em: 16 jun. 2020.

SENADO FEDERAL. **Carta Brasileira para Cidades Inteligentes.** 19 fev. 2020, Sec. CDR - Comissão de Desenvolvimento Regional e Turismo. Disponível em: shorturl.at/bmrY9 Acesso em: 16 jun. 2020.

SOPRANA, P. Plano de incentivo à conectividade no país está na geladeira. **Folha de São Paulo**, 2 fev. 2019.

SUNSTEIN, C. R. **Nudging: A Very Short Guide**. Rochester, NY: Social Science Research Network, 22 set. 2014. Disponível em: https://papers.ssrn.com/abstract=2499658. Acesso em: 4 jul. 2020.

TAUTE, F. Reconhecimento Facial e suas controvérsias. **Heinrich-Böll-Stiftung**, 7 fev. 2020. Disponível em: shorturl.at/adpzQ. Acesso em: 30 jun. 2020.

UN-HABITAT. **The Strategic Plan 2020-2023**. Nairobi: United Nations Human Settlements Programme, 2019.

UNITED NATIONS. **Human Rights Council Resumes Its Forty-Third Session And Holds a General Debate on Human Rights Bodies And Mechanisms**. . In: U.N. HUMAN RIGHTS COUNCIL. Geneva: 15 jun. 2020. Disponível em: shorturl.at/djGMZ. Acesso: 30 jun. 2020.

UNODC. **United Nations Office on Drugs and Crime: Homicide**. [s.l.] United Nations, 2019. Disponível em: https://dataunodc.un.org/#state:1. Acesso em: 10 jun. 2020.

WEBER, R. H. Internet of things – Governance quo vadis? **Computer Law & Security Review**, v. 29, n. 4, p. 341–347, ago. 2013.

WORLD ECONOMIC FORUM. **The Global Competitiveness Report 2019**. Geneva: WEF, 2019.

WRI BRASIL. **O que são cidades inteligentes no Brasil e como elas podem promover o desenvolvimento sustentável | WRI Brasil**, 13 fev. 2020. Disponível em: https://wribrasil.org.br/en/node/44594. Acesso em: 4 jul. 2020

Anexo 1 – Câmara IoT

Relação de membros que compõem a Câmara IoT (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 2020b):

1. Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC
2. Ministério da Indústria, Comércio Exterior e Serviços – MDIC
3. Ministério dos Transportes, Portos e Aviação Civil – MTPA
4. Ministério da Agricultura, Pecuária e Abastecimento – MAPA
5. Ministério do Planejamento, Desenvolvimento e Gestão – MPDG
6. Ministério da Defesa – MD
7. Ministério das Cidades – MCID
8. Ministério das Relações Exteriores – MRE
9. Casa Civil da Presidência da República
10. Câmara dos Deputados
11. Banco Nacional de Desenvolvimento Econômico e Social – BNDES
12. Financiadora de Estudos e Projetos – FINEP
13. Agência Nacional de Telecomunicações – ANATEL
14. Agência Nacional de Transportes Aquaviários – ANTAQ
15. Agência Brasileira de Desenvolvimento Industrial – ABDI
16. Agência Brasileira de Promoção de Exportações e Investimentos – APEX
17. Empresa Brasileira de Pesquisa e Inovação Industrial – EMBRAPII
18. Empresa Brasileira de Pesquisa Agropecuária – EMBRAPA
19. Empresa de Planejamento e Logística S.A. – EPL
20. Rede Nacional de Ensino e Pesquisa – RNP
21. Comitê Gestor da Internet no Brasil - CGI.br
22. Associação Brasileira de Prefeituras – ABRAP
23. Frente Nacional de Prefeitos – FNP
24. Associação Brasileira de Municípios - ABM
25. Universidade de São Paulo – USP
26. Universidade Federal do Rio de Janeiro – UFRJ
27. Universidade de Brasília – UnB
28. Centro de Estudos em Telecomunicações - CETUC/PUC-RJ
29. Instituto Nacional de Telecomunicações – INATEL
30. Universidade Federal de Pernambuco – UFPE
31. Laboratório Nacional de Redes de Computadores – LARC

32. Centro de Pesquisa e Desenvolvimento em Telecomunicações – CPqD
33. Centro de Estudos e Sistemas Avançados do Recife – CESAR
34. Instituto de Pesquisas Eldorado
35. FITec - Inovações Tecnológicas
36. Fundação Centros de Referência em Tecnologias Inovadoras – CERTI
37. Associação para Promoção da Excelência do Software Brasileiro – SOFTEX
38. Fórum Brasileiro de Internet das Coisas
39. Sociedade Brasileira de Computação – SBC
40. Sociedade Brasileira de Microeletrônica – SBMICRO
41. Associação Brasileira Científica para Inovação – ABCI
42. Instituto Brasileiro de Defesa do Consumidor - IDEC
43. Confederação Nacional da Indústria – CNI
44. Confederação Nacional da Agricultura – CNA
45. Confederação Nacional do Comércio – CNC
46. Confederação Nacional da Tecnologia da Informação e Comunicação – ConTIC
47. Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal – SINDITELEBRASIL
48. Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação – BRASSCOM
49. Associação Brasileira da Indústria Elétrica e Eletrônica – ABINEE
50. Associação de Empresas do Setor Eletroeletrônico de Base Tecnológica Nacional - P&D Brasil
51. Associação Brasileira da Indústria de Semicondutores – ABISEMI
52. Associação Brasileira das Empresas de Software – ABES
53. Associação Brasileira da Indústria Têxtil e de Confecção – ABIT
54. Associação Brasileira de Internet das Coisas – ABINC
55. Associação Brasileira de Internet Industrial – ABII
56. Associação Brasileira de Automação - GS1 Brasil
57. Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança - ABESE
58. Associação Catarinense de Tecnologia - ACATE
59. Sindicato Nacional das Empresas de Telecomunicações por Satélite – SINDISAT
60. Associação Nacional dos Fabricantes de Veículos Automotores – ANFAVEA
61. Groupe Speciale Mobile Association - GSMA Brasil
62. Utilities Telecom & Technology Council America Latina – UTCAL
63. BSA - The Software Alliance
64. Associação Brasileira de Provedores de Internet e Telecomunicações - ABRINT
65. Laboratório de Sistemas Integráveis Tecnológico - LSITEC

Anexo 2 – Investimentos BNDES

Extratos do sistema "Consulta a operações do BNDES" (2020) relativos aos investimentos no estudo "Internet das Coisas: um plano de ação para o Brasil" (BNDES, 2017d) e no programa BNDES Pilotos IoT (2018a).

Quadro 21: Consulta a operações do BNDES

MCKINSEY & COMPANY INC DO BRASIL CONSULTORIA LTDA

Contrato	Data	Valor contratado (R$)	Situação	Tipo da operação
16207131	06/01/2017	6.726.987	LIQUIDADO	NÃO AUTOMÁTICA

Descrição: REALIZACAO DE ESTUDO TECNICO INDEPENDENTE COM OBJETIVO DE ELABORAR UM DIAGNOSTICO LOCAL E PROPOR POLÍTICAS PUBLICAS NO TEMA INTERNET DAS COISAS (INTERNET OF THINGS - IOT).

Forma de apoio	Fonte de Recursos	Valor desembolsado (R$)
DIRETA	RECURSOS ESTATUTÁRIOS - PRÓPRIOS ESTATUTÁRIOS	6.485.818

FUNDACAO CPQD - CENTRO DE PESQUISA E DESENVOLVIMENTO EM

Contrato	Data	Valor contratado (R$)	Situação	Tipo da operação
16207131	06/01/2017	2.246.720	LIQUIDADO	NÃO AUTOMÁTICA

Descrição: REALIZACAO DE ESTUDO TECNICO INDEPENDENTE COM OBJETIVO DE ELABORAR UM DIAGNOSTICO LOCAL E PROPOR POLÍTICAS PUBLICAS NO TEMA INTERNET DAS COISAS (INTERNET OF THINGS - IOT).

Forma de apoio	Fonte de Recursos	Valor desembolsado (R$)
DIRETA	RECURSOS ESTATUTÁRIOS - PRÓPRIOS ESTATUTÁRIOS	2.202.831

PEREIRA NETO, MACEDO ADVOGADOS

Contrato	Data	Valor contratado (R$)	Situação	Tipo da operação
16207131	06/01/2017	825.000	LIQUIDADO	NÃO AUTOMÁTICA

Descrição: REALIZACAO DE ESTUDO TECNICO INDEPENDENTE COM OBJETIVO DE ELABORAR UM DIAGNOSTICO LOCAL E PROPOR POLÍTICAS PUBLICAS NO TEMA INTERNET DAS COISAS (INTERNET OF THINGS - IOT).

Forma de apoio	Fonte de Recursos	Valor desembolsado (R$)
DIRETA	RECURSOS ESTATUTÁRIOS - PRÓPRIOS ESTATUTÁRIOS	793.305

FUNDACAO CPQD - CENTRO DE PESQUISA E DESENVOLVIMENTO EM

Contrato	Data	Valor contratado (R$)	Situação	Tipo da operação
19204751	18/11/2019	2.975.326	ATIVO	NÃO AUTOMÁTICA

Descrição: USO DE VISAO COMPUTACIONAL E CAMERAS DE ALTA DEFINICAO PARA SEGURANCA PUBLICA, PORTAIS DE RECONHECIMENTO E IDENTIFICACAODE VEICULOS PELO USO DE CAMERAS INTELIGENTES, ESTACOES METE OROLOGICAS COMPACTAS E CONECTADAS, PROVIMENTO DE SERVICO DEVEICULOS ELETRICOS COMPARTILHADOS, SERVICO DE ILUMINACAO PU BLICA POR MEIO DE PLATAFORMA DE TELEGESTAO CONVERGENTE.

Forma de apoio	Fonte de Recursos	Valor desembolsado (R$)
DIRETA	NÃO DISPONÍVEL	Não disponível

FUNDACAO INSTITUTO NACIONAL DE TELECOMUNICACOES

Contrato	Data	Valor contratado (R$)	Situação	Tipo da operação
19207651	31/01/2020	1.438.421	ATIVO	NÃO AUTOMÁTICA

Descrição
REALIZACAO DE EXPERIMENTOS DE SOLUCOES DE INTERNET DAS COISAS FOCADAS EM ILUMINACAO INTELIGENTE E VIDEOMONITORAMENTO, BEM COMO DIVULGACAO DE RELATORIO DE AVALIACAO DO PROJETO, NO AMBITO DO BNDES PILOTOS DE IOT

Forma de apoio	Fonte de Recursos	Valor desembolsado (R$)
DIRETA	NÃO DISPONÍVEL	Não disponível

ASSOCIACAO DO LABORATORIO DE SISTEMAS INTEGRAVEIS TECNO

Contrato	Data	Valor contratado (R$)	Situação	Tipo da operação
19206501	17/01/2020	2.626.790	ATIVO	NÃO AUTOMÁTICA

Descrição
REALIZAR EXPERIMENTOS DE SOLUCOES DE INTERNET DAS COISAS EM MOBILIDADE URBANA E VIGILANCIA URBANA NO MUNICIPIO DE SAO PAULO (SP), BEM COMO DIVULGAR RELATORIO DE AVALIACAO DO PROJETO, NO AMBITO DO BNDES PILOTOS DE IOT.

Forma de apoio	Fonte de Recursos	Valor desembolsado (R$)
DIRETA	NÃO DISPONÍVEL	Não disponível

Fonte: BNDES (2020)

Instituto Serzedello Corrêa

Missão

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo

Visão

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável

TRIBUNAL DE CONTAS DA UNIÃO