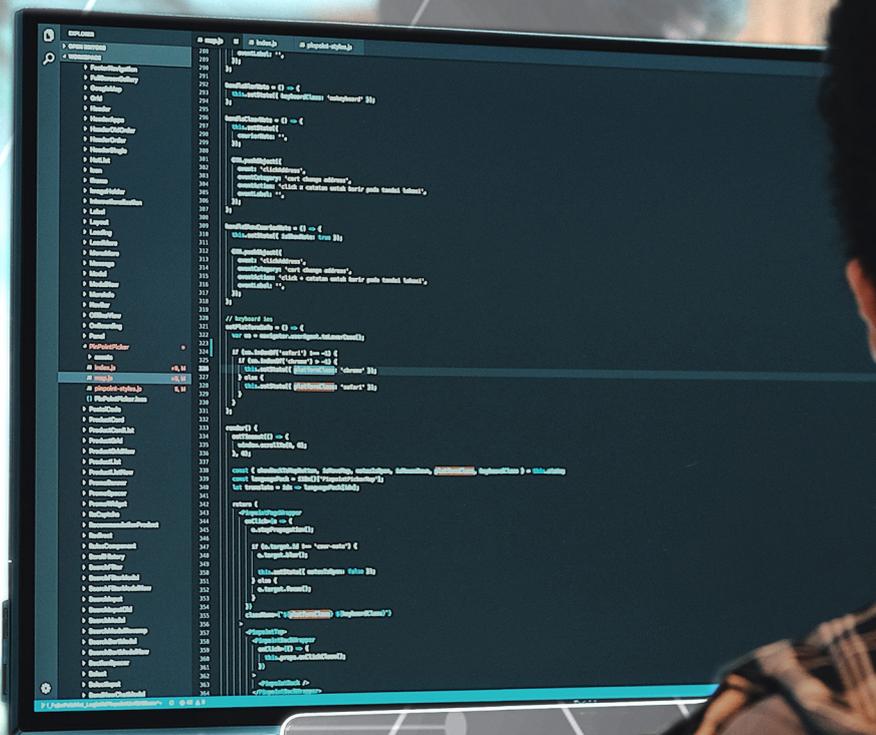


# FUNDAMENTOS DA CIÊNCIA DA COMPUTAÇÃO 2

ERNANE ROSA MARTINS  
(ORGANIZADOR)



Ernane Rosa Martins  
(Organizador)

# Fundamentos da Ciência da Computação 2

Atena Editora  
2019

2019 by Atena Editora  
Copyright © Atena Editora  
Copyright do Texto © 2019 Os Autores  
Copyright da Edição © 2019 Atena Editora  
Editora Executiva: Prof<sup>a</sup> Dr<sup>a</sup> Antonella Carvalho de Oliveira  
Diagramação: Lorena Prestes  
Edição de Arte: Lorena Prestes  
Revisão: Os Autores

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

### **Conselho Editorial**

#### **Ciências Humanas e Sociais Aplicadas**

Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas  
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília  
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa  
Prof<sup>a</sup> Dr<sup>a</sup> Cristina Gaio – Universidade de Lisboa  
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia  
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná  
Prof<sup>a</sup> Dr<sup>a</sup> Ivone Goulart Lopes – Istituto Internazionele delle Figlie de Maria Ausiliatrice  
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense  
Prof<sup>a</sup> Dr<sup>a</sup> Lina Maria Gonçalves – Universidade Federal do Tocantins  
Prof<sup>a</sup> Dr<sup>a</sup> Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof<sup>a</sup> Dr<sup>a</sup> Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa  
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará  
Prof<sup>a</sup> Dr<sup>a</sup> Vanessa Bordin Viera – Universidade Federal de Campina Grande  
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

#### **Ciências Agrárias e Multidisciplinar**

Prof. Dr. Alan Mario Zuffo – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano  
Prof<sup>a</sup> Dr<sup>a</sup> Daiane Garabeli Trojan – Universidade Norte do Paraná  
Prof. Dr. Darllan Collins da Cunha e Silva – Universidade Estadual Paulista  
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul  
Prof<sup>a</sup> Dr<sup>a</sup> Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia  
Prof. Dr. Jorge González Aguilera – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará  
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

#### **Ciências Biológicas e da Saúde**

Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás  
Prof.<sup>a</sup> Dr.<sup>a</sup> Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina  
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria  
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará

Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão  
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa  
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

### **Ciências Exatas e da Terra e Engenharias**

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto  
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

### **Conselho Técnico Científico**

Prof. Msc. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo  
Prof. Dr. Adaylson Wagner Sousa de Vasconcelos – Ordem dos Advogados do Brasil/Seccional Paraíba  
Prof. Msc. André Flávio Gonçalves Silva – Universidade Federal do Maranhão  
Prof.ª Drª Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico  
Prof. Msc. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro  
Prof. Msc. Daniel da Silva Miranda – Universidade Federal do Pará  
Prof. Msc. Eliel Constantino da Silva – Universidade Estadual Paulista  
Prof.ª Msc. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia  
Prof. Msc. Leonardo Tullio – Universidade Estadual de Ponta Grossa  
Prof.ª Msc. Renata Luciane Polsaque Young Blood – UniSecal  
Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista

<b>Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)</b>	
F981	Fundamentos da ciência da computação 2 [recurso eletrônico] / Organizador Ernane Rosa Martins. – Ponta Grossa (PR): Atena Editora, 2019. – (Fundamentos da Ciência da Computação; v. 2)  Formato: PDF Requisitos de sistema: Adobe Acrobat Reader Modo de acesso: World Wide Web Inclui bibliografia ISBN 978-85-7247-390-3 DOI 10.22533/at.ed.903192106  1. Computação – Pesquisa – Brasil. I. Martins, Ernane Rosa. CDD 004
<b>Elaborado por Maurício Amormino Júnior – CRB6/2422</b>	

Atena Editora  
Ponta Grossa – Paraná - Brasil  
[www.atenaeditora.com.br](http://www.atenaeditora.com.br)  
contato@atenaeditora.com.br

## APRESENTAÇÃO

A Ciência da Computação trouxe inúmeros benefícios para a sociedade moderna, tais como: a criação de empregos, o desenvolvimento de novos equipamentos e até mesmo o ganho de produtividade nas empresas. Proporcionou também facilidades inerentes ao acesso a informação, como: a internet, as redes sociais, os buscadores e os aplicativos móveis. Os estudos oriundos da Ciência da Computação são aplicados em diversas áreas do conhecimento, utilizados na resolução de diferentes problemas da sociedade, trazendo avanços significativos para a vida de inúmeras pessoas ao redor do mundo.

Assim, esta obra permite o contato com os resultados de trabalhos recentes realizados por autores de diversas instituições brasileiras, onde são abordados assuntos importantes desta área, tais como: realidade aumentada; jogos sérios; processamento de linguagem natural; uso de tecnologias e cognição humana; inteligência artificial; ciberespaço; digitalização do espaço; ciborguização do ser humano; interação com dispositivos digitais; cultura pop como ferramenta de ensino; computação em nuvem; transformações do ambiente digital; interação humano-computador nos dispositivos digitais, realidade virtual e aplicativos 3D; uso da criptografia; internet das coisas e cidades inteligentes; inclusão na sociedade da informação e da cibercultura; tipografia por meio de interfaces digitais; surgimento e evolução das techs em território brasileiro; e redes sociais conectadas.

Por tanto, espera-se que este livro venha a ajudar tanto aos alunos dos cursos superiores de Ciência da Computação quanto aos profissionais atuantes nesta importante área do conhecimento. Desejo a todos uma ótima leitura e que esta obra contribua de forma relevante para o seu aprendizado.

Ernane Rosa Martins

## SUMÁRIO

<b>CAPÍTULO 1</b> .....	<b>1</b>
USO DA REALIDADE AUMENTADA NO AUXÍLIO DO ENSINO DE SÓLIDOS GEOMÉTRICOS E GEOMETRIA MOLECULAR	
Matheus Alencar de Medeiros Lucena Éverton Rômulo S. Castro	
DOI 10.22533/at.ed.9031921061	
<b>CAPÍTULO 2</b> .....	<b>9</b>
UMA PROPOSTA DE APLICAÇÃO DE JOGOS SÉRIOS PARA AUXILIAR NA IDENTIFICAÇÃO DE DISLEXIA E DISLALIA EM CRIANÇAS	
Arthur Costa Gorgônio Karlíane Medeiros Ovidio Vale Flavius da Luz e Gorgônio Rodrigo Valença Cavalcante Frade	
DOI 10.22533/at.ed.9031921062	
<b>CAPÍTULO 3</b> .....	<b>20</b>
TÉCNICAS DE PROCESSAMENTO DE LINGUAGEM NATURAL PARA ANÁLISE E CLASSIFICAÇÃO DE SENTIMENTOS UTILIZANDO FILTRAGEM POR <i>EMOJI</i>	
Ariana Moura da Silva Rodrigo da Mattas Bastos Ricardo Luis de Azevedo da Rocha	
DOI 10.22533/at.ed.9031921063	
<b>CAPÍTULO 4</b> .....	<b>26</b>
PROGRAMA EXTENSIONISTA DE CORO INFANTIL EM SÍTIO ELETRÔNICO E SEU REFLEXO NO FORTALECIMENTO DA INTERAÇÃO DIALÓGICA	
Débora Andrade Wesley Jesus dos Santos Anna Luíza Batista Santos Talisson Samuel Silva	
DOI 10.22533/at.ed.9031921064	
<b>CAPÍTULO 5</b> .....	<b>35</b>
PRIVACIDADE / EVASÃO: O SUJEITO COMO PRODUTOR DE CONTEÚDO E EVASOR DA PRÓPRIA INTIMIDADE	
Lucilene Cury Maurício Barbosa da Cruz Felício	
DOI 10.22533/at.ed.9031921065	
<b>CAPÍTULO 6</b> .....	<b>48</b>
OS SMARTPHONES COMO EXTENSÕES DA MENTE: HIBRIDAÇÃO, ACOPLAMENTO E COGNIÇÃO	
Camila Moura Pinto	
DOI 10.22533/at.ed.9031921066	
<b>CAPÍTULO 7</b> .....	<b>53</b>
O PRECONCEITO NAS MÁQUINASTHE PREJUDICE IN THE MACHINES	
Marcus Antonio de Lyra Alves	
DOI 10.22533/at.ed.9031921067	

<b>CAPÍTULO 8</b> .....	<b>67</b>
O CIBERESPAÇO COMO PLATAFORMA DE DIVULGAÇÃO E MOBILIZAÇÃO DE PESSOAS PARA EVENTOS AMBIENTAIS REALIZADOS NO BRASIL	
Nathalia Baldini Inson Adriana Rodrigues José Roberto Madureira Júnior	
<b>DOI 10.22533/at.ed.9031921068</b>	
<b>CAPÍTULO 9</b> .....	<b>79</b>
NET-ATIVISMO NA AMAZÔNIA EM DEFESA DE UMA ECOLOGIA DA COMUNICAÇÃO	
Ian Victor Santana Dawsey	
<b>DOI 10.22533/at.ed.9031921069</b>	
<b>CAPÍTULO 10</b> .....	<b>90</b>
MENTES, ALGORITMOS, CIBORGUES E A AUTOMAÇÃO DE CONTEÚDOS A SOCIEDADE CIBORGUE: OS IMPACTOS DAS TECNOLOGIAS DIGITAIS NO INDIVÍDUO CONTEMPORÂNEO	
Bruno Antunes	
<b>DOI 10.22533/at.ed.90319210610</b>	
<b>CAPÍTULO 11</b> .....	<b>103</b>
DIGITAL DATING – PERFIL DAS ESTRATÉGIAS DE NAMORO EM PLATAFORMAS DIGITIAS	
Guaracy Carlos da Silveira Marina Silva Tavares	
<b>DOI 10.22533/at.ed.90319210611</b>	
<b>CAPÍTULO 12</b> .....	<b>116</b>
COMPUTAÇÃO EM NUVEM: PLATAFORMA COMO SERVIÇO	
Thiago Martins Pereira Adani Cusin Sacilotti José Roberto Madureira Júnior	
<b>DOI 10.22533/at.ed.90319210612</b>	
<b>CAPÍTULO 13</b> .....	<b>126</b>
CALCMEMORIAL - APLICATIVO JAVA PARA A ELABORAÇÃO DE MEMORIAIS DESCRITIVOS DE IMÓVEIS RURAIS	
Victor da Cruz Peres Fabrício de Sousa Ribeiro Enéias Monteiro da Silva Emerson Cordeiro Morais	
<b>DOI 10.22533/at.ed.90319210613</b>	
<b>CAPÍTULO 14</b> .....	<b>139</b>
ATORES EM REDE NA PRODUÇÃO DE CONTEÚDO: REFLEXÕES SOBRE EMPRESAS INFORMATIVAS E GESTÃO DO RELACIONAMENTO COM PROSUMERS NAS MÍDIAS SOCIAIS	
Rafael Vergili Fabiana Grieco Cabral de Mello Vetritti	
<b>DOI 10.22533/at.ed.90319210614</b>	
<b>CAPÍTULO 15</b> .....	<b>150</b>
ANÁLISE DO DESENVOLVIMENTO DE UM JOGO DE LÓGICA EM DISPOSITIVOS PARA REALIDADE VIRTUAL E APLICATIVOS 3D	
Lucy Mari Tabuti	

Ricardo Nakamura

DOI 10.22533/at.ed.90319210615

**CAPÍTULO 16 ..... 168**

A RESISTÊNCIA CONTRA A VIOLAÇÃO DA PRIVACIDADE NA ERA DAS TECNOLOGIAS *SMART*:  
O USO DA CRIPTOGRAFIA COMO FERRAMENTA DE EMBATE POLÍTICO

Bruno Antunes

DOI 10.22533/at.ed.90319210616

**CAPÍTULO 17 ..... 184**

A PRIVACIDADE EM UM CENÁRIO *PANSENSITÍVEL* DE INTERNET DAS COISAS & CIDADES  
INTELIGENTES

André Barbosa Ramiro Costa

Maria Amália Oliveira de Arruda Câmara

DOI 10.22533/at.ed.90319210617

**CAPÍTULO 18 ..... 197**

A PARCERIA PAITER-SURUÍ E *GOOGLE INC.*: A FLORESTA EM REDE, UM ESTUDO DE CASO

Walace Soares de Oliveira

Marco Antônio de Almeida

DOI 10.22533/at.ed.90319210618

**CAPÍTULO 19 ..... 209**

A GESTUALIDADE INCORPORADA NA TIPOGRAFIA POR MEIO DE INTERFACES DIGITAIS

Karine Itao Palos

DOI 10.22533/at.ed.90319210619

**CAPÍTULO 20 ..... 221**

A ERA DAS TECHS E A HIBRIDIZAÇÃO DOS NEGÓCIOS

Siméia de Azevedo Santos

DOI 10.22533/at.ed.90319210620

**CAPÍTULO 21 ..... 236**

#HOMOFOBIAÉDOENÇA: ATIVISMO LGBT NOS AMBIENTES DIGITAIS CONTRA A “CURA GAY”

Augusto Rafael Brito Gambôa

DOI 10.22533/at.ed.90319210621

**SOBRE O ORGANIZADOR..... 248**

## A PRIVACIDADE EM UM CENÁRIO *PANSENSITÍVEL* DE INTERNET DAS COISAS & CIDADES INTELIGENTES

**André Barbosa Ramiro Costa**

Universidade Federal de Pernambuco - UFPE

**Maria Amália Oliveira de Arruda Câmara**

Universidade de Pernambuco - UPE

**RESUMO:** A expansão do ecossistema da Internet das Coisas (IoT), sobretudo em um contexto de Cidades Inteligentes, tem como pano de fundo as bases técnicas do funcionamento da IoT, porém aponta para questões políticas como os desafios à privacidade e a expansão da vigilância. Essas relações convergem para uma discussão político-acadêmica que sugere a necessidade de um programa de proteção de dados pessoais e garantia de direitos fundamentais, mediante a construção legislativa. Dá-se como ponto de partida, no contexto brasileiro, a Lei Geral de Proteção de Dados brasileira, bem como leva-se em consideração as dinâmicas de uma Governança da Internet e a participação da sociedade civil. Este artigo procura iluminar pontos sobre os riscos à privacidade em um ambiente de cidades inteligentes, quais os interesses econômicos, para além da melhoria dos serviços urbanos, na captura de dados. Por fim, o artigo explora se o marco legislativo de proteção de dados pessoais brasileiro seria suficiente para garantir direitos fundamentais em uma realidade de sensores.

**PALAVRAS-CHAVE:** internet das coisas; cidades inteligentes; privacidade; proteção de dados; vigilância.

**ABSTRACT:** The expansion of the Internet of Things (IoT) ecosystem, especially in a context of Smart Cities, has as background the technical bases of IoT's operation, but points to political issues such as the challenges to privacy and the expansion of surveillance. These relations converge to a political-academic discussion that suggests the necessity of a program to protect personal data and defend fundamental rights, through a legislative approach. The starting point, in the brazilian context, is the General Data Protection Law as well as the dynamics of an Internet Governance and the participation of civil society. This paper intends to illuminate issues about risks to privacy in a smart cities environment as well as economic interests in data collection beyond the improving of urban services. At last, the paper explores if the brazilian legislative data protection framework is enough to guarantee fundamental rights in a sensors reality.

**KEYWORDS:** internet of things; smart cities; privacy; data protection; surveillance.

### 1 | EXPANSÃO DAS COISAS E DAS CIDADES

## CONECTADAS

A disseminação e o crescimento da capacidade computacional dos dispositivos não se restringem apenas aos atuais computadores pessoais e aos aparelhos móveis. O poder de processamento de informações vem alcançando o próprio meio ambiente, os objetos pessoais, os corpos e as próprias cidades, caracterizando um fenômeno que se convencionou chamar de Internet das Coisas (Internet of Things ou IoT).

O batismo da referida tecnologia é comumente creditada a uma apresentação de negócios, em 1999 feita por Kevin Ashton. O pioneiro tecnólogo, na oportunidade, sugeriu que os computadores - e a Internet - eram, então, dependentes de seres humanos para coletar informações, fator este que, acreditava, não carregava um nível de aproveitamento otimizado, pois os seres humanos possuem limitações motoras e de tempo para digitar, cadastrar ou scannear os dados necessários. Sugeria então que computadores fossem desenvolvidos de modo a poderem coletar e processar informações, através de sensores, sem necessitarem da intervenção ou do monitoramento “limitado” do ser humano (ASHTON, 2009).

Na realidade, a primeira notícia de um dispositivo conectado à Internet é datado de muito antes da criação do termo por Kevin Ashton. Programadores do departamento de Ciência da Computação, na Universidade de Carnegie Mellon, na década de 70, conectaram uma máquina de Coca-Cola à rede, sendo esse o mais remoto registro de um objeto conectado que que não fosse um computador. Desde então, a ideia de uma tecnologia que possibilitasse a comunicação entre máquinas, machine-to-machine, vem alimentando o conceito da computação ubíqua, inaugurado por Mark Weiser (1988), uma realidade onde computadores estivessem onipresentes, com tarefas específicas e inter-comunicandas.

Ou seja, ainda que haja uma longa história a respeito do desenvolvimento de IoT, apenas recentemente veio saltar aos olhos da comunidade não especializada. Hoje, a IoT excede, em quantidade, o número de pessoas, segundo dados da Federal Trade Commission (2015).

A Pew Reserch Center define a IoT como

“um ambiente de computação em rede, global, imersivo e invisível, construído através de proliferação continuada de sensores inteligentes, câmeras, softwares, base de dados e massivos data centers em um tecido de informação em expansão mundial” (ANDERSON, RAINE, 2014).

Levantamento da CISCO (2011) estima que cerca mais de 50 bilhões de coisas estarão conectadas em 2020. Essa perspectiva inclui objetos domésticos, tais como geladeiras e fogões, bem como objetos urbanos, de uso comum, tais como semáforos, lixeiras e barômetros. É possível entender, então, que as IoT estarão atreladas ora ao uso pessoal, no ambiente doméstico, ora ao público, nas cidades e espaços coletivos.

Não há melhor paradigma destes espaços comuns do que as próprias cidades. Estas, por sua vez, vêm carregando graus de conectividade e poder computacional

crescentes, atrelados ao funcionamento de serviços públicos. Essa nova dimensão de conectividade vem caracterizando o que se convencionou chamar, pelo setor empresarial, de “cidades inteligentes”.

A IBM (2018) a define como “novas formas de funcionamento para as cidades”. Para a Sidwalk Labs (2018), empresa pertencente à Alphabet, são “novos tipos de lugares que aceleram a inovação urbana” e a CISCO (2018) enxerga como “a cidade elevando a forma como as pessoas se conectam e interagem com as cidades”. Esse mercado constitui um trend tecnológico conveniente, carregado, sobretudo, pelas grandes empresas de tecnologia que estarão à frente da produção e comercialização, tendo em vista uma previsão de crescimento de 424.68 bilhões de dólares, em 2017, para mais de 1.201 bilhões de dólares em 2022 (MARKETS AND MARKETS, 2018).

Porém, para além do discurso do marketing, faz necessário observar o fenômeno das cidades inteligentes sob o viés do mercado de dados. Cidades inteligentes, então, podem ser vistas como a coleta de dados, no espaço público, por parte do governo e do setor privado, para oferecer serviços (PRIVACY INTERNATIONAL, 2018).

Neste contexto, pode-se encarar a expansão da conectividade dos dispositivos, relacionados às cidades ou não, como a expansão da coleta de dados, em termos de volume, variedade de tipos de dados e velocidade, compondo os elementos do processamento de dados conhecido como big data.

Dispositivos e cidades conectadas implicam uma maior coleta de dados pessoais, conseqüentemente. Esta afirmação caracteriza uma maior fragilidade do cidadão em relação a sua privacidade, uma vez que esta ubiquidade computacional, através de sensores, pode servir a exponenciar o sistema de monitoramento dos cidadãos. Pode-se assumir que a perda da privacidade em espaços públicos acarreta conseqüências à liberdades civis e nega chances de dissidências ou protestos, por exemplo (PRIVACY INTERNATIONAL, 2018).

Políticas econômicas estabelecidas por parte dos entes estatais, em parcerias público-privadas, afetam a forma como os cidadãos interagem com o ambiente urbano, uma vez que informações estão sendo mercantilizadas e geridos em uma governança de dados pessoais que não envolve a sociedade civil em sua construção.

## **2 | A PRIVACIDADE NA CIDADE PANSENSITÍVEL**

A mudança nas dinâmicas do funcionamento das cidades, para além dos serviços públicos urbanos, influenciam o próprio comportamento dos cidadãos, suas escolhas, a forma como interage com a cidade, a forma como se associa coletivamente, onde está presente, com quem está reunido ou os trajetos que toma.

Essa realidade não traz novidade quando se tratando da auto-restrição de comportamentos do sujeito ao estar online. Diferente da mentalidade do início do século XXI, quando a experiência online carregava um grau de não-identificação, a atmosfera

da Internet, hoje, vem acompanhada de desconfiança e insegurança. Diariamente, notícias a respeito de programas de vigilância em massa, operadas por Estados e grande monopólios tecnológicos, vem alimentando uma verdadeira paranoia coletiva.

Revelação sobre a existência de programas de espionagem, a qual pôs em xeque o sentimento de privacidade na Internet, se deram como no caso do já notório whistleblower Edward Snowden, em 2013, quando este, ex-funcionário terceirizado da NSA, revelou a existência de uma coleta de dados massiva, de forma indiscriminada e generalizada, de cidadãos de todo o mundo, incluindo alvos estratégicos, como chefes de Estado. Casos de revelações sobre programas de vigilância em massa não são tão recentes e vêm sendo noticiados muito antes do caso Snowden. William Binney, criptoanalista e também ex-funcionário da NSA, ainda em 2002 já havia alertado sobre programas de vigilância em massa operados pelos Estados Unidos, como o programa Trailblazer, sistema cuja função era analisar dados massivos de celulares e e-mails. Como Binney e Snowden, outros whistleblowers foram notáveis em revelar programas de espionagem estatal, como Thomas Drake e John Crane, contrubindo para a construção de uma atmosfera de desconfiança no ciberespaço. Em se tratando de novos níveis de conexão e novos dispositivos, isso implica dizer que maiores níveis de vigilância também virão à reboque.

Grande parcela dos dispositivos de IoT são construídos com um propósito básico: monitorar a atividade humana. “Consciência” sobre o ambiente através de sensores de áudio, imagem, dados de localização e outras formas de detecção são objetivos centrais. Ainda que a qualidade de novos serviços de detecção venham a oferecer melhorias nas atividades diárias, não há dúvidas sobre os impactos à privacidade: o usuário estará, exponencialmente, sob observação pelas suas próprias máquinas e dispositivos pessoais.

A “invisibilidade” destes serviços - into the fabric of daily life until they are indistinguishable from it (WEISER, 1988) – torna suas consequências políticas imperceptíveis para os usuários. Em contraste, quando cedemos informações a plataformas online, tal como Facebook, Amazon ou Google, tem-se minimamente a consciência sobre o uso ou a permanência nos domínios da plataforma. Em um contexto de IoT, a escolha e oportunidade de consentir ou não são ausentes by design. Ou seja, dispositivos de IoT, em sua maioria, não oferecem alertas sobre políticas de privacidade ou criam interfaces para o consentimento ajustados à interação com usuário.

Aprofunda-se o problema, certamente, quando se tratando de cidades inteligentes, repletas de sensores. Lixeiras, metrô ou postes de luz inteligentes não oferecem qualquer oportunidade para o titular das informações coletadas expressar suas escolhas.

Não bastando não haver opt-out quando do “uso” destes serviços, também não há o mero conhecimento sobre a coleta de dados. Na cidade de Londres, lixeiras inteligentes foram instaladas em 2012, coletando dados dos cidadãos para direcionar

propagandas. Não havia conhecimento sobre a coleta dos dados ou, muito menos, sobre a finalidade desta coleta (DATOO, 2013).

Em algumas nações, o uso de dados de cidadãos coletados pelos governos já sugere que a redução de privacidade serve a interesses políticos e não, necessariamente, a melhorias na qualidade de vida urbana. Na China, tecnologias de big data, somadas à vigilância em massa estatal dão um bom exemplo de como sensores urbanos podem alimentar a violação de direitos humanos. Nesse caso, realizam previsão de protestos ou manifestações através do mapeamento de aglomerações (MURDOCK, 2016).

Esses casos e outros similares redesenham a interação humano-espço público. Se, por um lado o reconhecimento e a identificação em relação ao bairro ou à cidade são elementos importantes na formação do senso de pertencimento e comunidade, certo grau de anonimato, diante da diversidade de pessoas, garante uma jornada diária única, rumo a novos espaços, novas pessoas e novas experiências, mesmo que na mesma área. É uma característica necessária à vida em grandes centros. Jane Jacobs (1961), escritora americana, reconhecida por seu ativismo quanto a temas relativos a direitos urbanos, em *Morte e Vida de Grande Cidades*, assinala que

“uma boa vizinhança urbana consegue um equilíbrio e tanto entre a determinação das pessoas de ter um mínimo de privacidade e seu desejo concomitante de poder variar os graus de contato, prazer e auxílio mantidos com as pessoas que as rodeiam”.

Hoje, podemos falar em pessoas e dispositivos que as rodeiam.

A privacidade não se confunde, conceitualmente, com informações ou dados pessoais. Porém, ao tomar uma delas por objeto, lida-se diretamente com a outra, como um ato reflexo, por uma equação simples que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa (DONEDA, 2011). A coleta e o processamento de dados através de sensores impactam, diretamente, a formação do indivíduo e da coletividade.

Ainda que o conceito de privacidade não seja cristalizado, sendo, inclusive, naturalmente desenvolvido e condicionado ao estado da tecnologia de cada época e sociedade (DONEDA, 2006), Alan West (1968) definiu a privacidade como o direito do indivíduo, grupos ou instituições de determinar, por si mesmos, quando, como e qual informação pessoal será comunicada a outros.

No contexto presente, o professor Daniel Solove (2006) estabelece uma categorização das atividades potencialmente nocivas à plenitude da privacidade. Aqui, pode-se levar em conta o estado da arte em mineração de dados, big data ou algoritmos de inteligência artificial. Então, segundo Solove, (1) a coleta de informações, ou seja, a vigilância, entendida como a observação, a escuta ou gravação das atividades de um indivíduo; e (2) a forma que a informação é armazenada, manipulada ou utilizada, no que resumiu por *processamento da informação*. Solove ramifica essa última em: agregar informação, ou seja, combinar uma série de dados sobre uma pessoa; *identificar* ou unir informações sobre indivíduos particulares; *não assegurar* que as informações

estejam armazenadas de forma eficiente; *usar alternativamente*, quer dizer, utilizar para outros fins que não os inicialmente anunciados; ocultar quais informações sobre o titular dos dados estão armazenadas, excluindo-o da relação.

Diante dos interesses empresariais, com atuação crescente de Data Brokers, o uso alternativo de dados também se faz presente, tendo em vista um mercado obscuro e não regulado, o qual opera mediante verdadeiro capitalismo (ZUBOFF, 2015) ou arquitetura (SCHNEIER, 2015) de vigilância. Sendo assim, as fronteiras entre IoT e vigilância podem se confundir e, em última análise, desaparecer caso iniciativas de proteção à privacidade não sejam levadas à cabo.

### 3 | O CENÁRIO PANSENSÍVEL NA PERSPECTIVA DE UMA LEI DE PROTEÇÃO DE DADOS PESSOAIS

Quando se tratando das dificuldades de manifestação de vontade ou acordo com os termos de coleta de dados dos dispositivos, a falta de regulação, a nível nacional e local, enfraquece ainda mais a garantia de direitos dos usuários dos serviços de IoT.

A Lei de Proteção de Dados Pessoais - LGPD, recentemente aprovada no Brasil, irá modificar as dinâmicas de coleta de dados de forma radical, visando uma maior tutela da privacidade. Aqui, falaremos especificamente das interfaces da Lei com dispositivos de IoT no que se refere à conceituação de dados pessoais, ao consentimento e aos dados anônimos.

Primeiramente, importante pensar sobre a abrangência do que será entendido por dados pessoais. A LGPD, tendo em vista a necessidade de sustentação constante e flexível da legislação diante do desenvolvimento tecnológico, adota o conceito expansionista sobre o que são dados pessoais. Disciplina, em seu art. 5º, inciso I, que dado pessoal é aquela informação relacionada à pessoa natural identificada ou identificável. Esse conceito, de herança doutrinária na *General Data Protection Regulation* europeia, engloba, igualmente, os dados com *potencial identificador* de um indivíduo, possuindo teor mais realista diante do atual - e futuro - poder de processamento de dados, sejam estruturados ou não. Em um contexto de cidade inteligente, um sensor acoplado a certo serviço pode ser programado para coletar dados que, ainda que não vincule o indivíduo imediatamente, pode gerar bancos de dados que, se cruzados com outros, possuirão o potencial de identificá-lo.

Outra proposta-chave trazida pela LGPD é referente aos dados anônimos. Estes seriam, basicamente, o contrário do dado pessoal, uma informação que não identifica uma pessoa específica. No texto da Lei, em art. 5º incisos III e XI, respectivamente, dados anonimizados são aqueles “relativos a um titular que não possa ser identificado”, enquanto que a anonimização será a “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”.

Hoje, diante das técnicas de re-identificação ou deanonimização, já é possível dizer que não existem mais dados anônimos (DONEDA, 2016). Cabe, então, sugerir que a mera coleta de dados por parte dos sensores em cidades inteligentes, sob promessa de anonimização, configura uma proteção frágil. O que ocorre, na maioria dos casos, ainda permite que determinado dado seja individualizado e cruzado com outros bancos de dados. É considerado raro que os dados produzidos pela atividade do usuário sejam completamente e irreversivelmente anonimizados (FUSTER, SCHERRER, 2015), o que pode sugerir um desafio futuro à implementação e *enforcement* da legislação.

O anonimato protege pessoas de preconceitos baseados em sua identidade e as possibilita de votar, expressarem-se e se associarem livremente, protegendo-as do perigo de represálias. Ainda pode facilitar a compreensão das ideias de outra pessoa, assim como a identificação pode causar pré-julgamentos. Torna possível que as pessoas sejam hábeis de criticar as empresas para as quais trabalham e a denunciá-las, bem como as protege de serem julgadas ao consumirem ideias não tão populares. Dessa forma, facilita a liberdade de expressão e a formação da identidade, livre de interferência ou de receios, fortalecendo a privacidade. O grau de anonimização dos dados coletados., portanto, pode gerar efeitos diretos na forma como o sujeito se relaciona com a sua comunidade, merecendo uma atenção ampla através da regulação.

O terceiro ponto, não menos importante, completando o que já foi chamado de tripé da proteção de dados pessoais (BIONI, 2015), é a figura do consentimento. Talvez esta seja a mais problemática quando se tratando de IoT nas cidades e da expressão de vontade usuários. A problemática do consentimento não é exclusiva da pauta de IoT ou de cidades inteligentes, mas é uma transversal à experiência do usuário dos serviços na Internet como um todo.

À luz da LGPD, em seu art. 5º, inciso XII, a manifestação do consentimento deve ser *livre, informada e inequívoca*, pela qual o titular concorda com o tratamento de seus dados pessoais para uma *finalidade determinada*. Entende-se estes elementos como, respectivamente: (1) não havendo nenhuma pressão ou coação sobre o titular dos dados; (2) o titular deve ter ciência sobre o que é o tratamento de dados pessoais e as implicações do tratamento; (3) não havendo dúvidas de que o titular consente com a prática do tratamento naquela situação; (4) e que se evite o consentimento genérico, obrigando a delimitação clara dos tipos de dados que serão alvo de tratamento (BANISAR, GUILLEMIN, BLANCO, 2016). Este arcabouço configura o que será nomeado de “autodeterminação informativa”, ou seja, o consumidor de um dispositivo conectado possui o direito de determinar como seus dados serão coletados e tratados (ZANATTA, 2017).

É levado a crer que a questão está na construção dos dispositivos, os quais não possuem, sequer, *displays* para que os titulares dos dados coletados possam expressar sua vontade. É possível dizer que uma “fadiga de consentimento” é imposta pela legislação de proteção de dados, por outro lado a garantia de direitos fundamentais,

tal como a privacidade, não pode ser vista como contrapeso ao processo inovador. Sendo assim, a ideia de *privacy by design* deve ser pensada desde o início do desenvolvimento da tecnologia. O design possui o potencial de empoderar as pessoas e sua relação com as tecnologias (IOT DESIGN MANIFESTO, 2015), desenvolvendo essa interação humano-máquina de forma aberta e livre de abusos.

#### 4 | GOVERNANÇA DA IOT E DAS CIDADES INTELIGENTES

A Internet das Coisas é um paradigma comunicacional ainda bastante recente e que causa algum estranhamento no momento de sua compreensão, regulação e governança. Para Caragliu et al. (2009) uma cidade pode ser considerada inteligente quando os investimentos em capital humano, social, tradicional, moderno, infraestrutura, comunicação, desenvolvimento econômico sustentável, qualidade de vida, gestão dos recursos naturais são soluções a partir da ação participativa e do engajamento de cidadãos. O conceito de cidade inteligente significa, portanto, a preocupação com a eficiência das ações humanas baseada na gestão inteligente das Tecnologias da Informação e Comunicação integradas com a participação ativa do cidadão. O resultado disso é um novo tipo de governança, fortemente centrada na participação cidadã nas políticas públicas.

Em uma pesquisa seminal coordenada pelo Centro de Ciências Regionais na Universidade de Tecnologia de Viena, foram identificados seis principais “eixos” ou “dimensões” característicos de cidades inteligentes, onde foram avaliadas 70 cidades europeias (GIFFINGER et al, 2007). Esses eixos são usados até hoje para as principais definições de cidades inteligentes, sendo eles: economia inteligente; mobilidade inteligente; ambiente inteligente; pessoas inteligentes; qualidade de vida inteligente; e, finalmente, destacamos uma governança inteligente. Os eixos são baseados, respectivamente, em teorias de competitividade regional, transportes e economia no uso das TICs, recursos naturais, capital humano e social, qualidade de vida e, principalmente, participação das sociedades nas cidades. Isso oferece uma base suficientemente sólida para a própria definição teórica de governança de IoT em cidades inteligentes.

A governança, partindo de uma perspectiva referencial europeia, refere-se às regras, processos, comportamentos à forma como os poderes são exercidos, particularmente levando-se em conta o grau de abertura, participação, prestação de contas, efetividade e coerência. Tais princípios também são corroborados pelas dinâmicas da Governança da Internet nos âmbitos da Internet Engineering Task Force - IETF, World Wide Web Consortium - W3C, ICANN e Internet Society, por exemplo, importantes players do ecossistema da Internet. Posto de outra forma, a Governança da Internet é o desenvolvimento e aplicação por governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios comuns, normas, regras,

procedimentos de tomada de decisão e programas que moldam a Internet (WORKING GROUP ON INTERNET GOVERNANCE, 2016). Importante, portanto, estender tais princípios ao contexto da IoT, afinal a tecnologia irá possibilitar que tudo se conecte à Internet, carregando, também, desafios à governança.

Não poderíamos, atualmente, dissociar a Governança da Internet de uma abordagem multissetorial, valor tão caro às rodadas de diálogo que constroem determinações, regulações e resoluções cruciais ao bom funcionamento da rede. Por um viés multissetorial, a governança deve ser construída através de processos democráticos, assegurando a participação significativa e responsável de todos os intervenientes, incluindo governos, setor privado, sociedade civil, a comunidade técnica, a comunidade acadêmica e usuários, devendo os respectivos papéis e responsabilidades das partes interessadas serem interpretados de modo flexível em relação aos temas em discussão (NETMUNDIAL, 2014).

Diante de uma variedade de atores interessados, os interesses por vezes entram em conflito diante de uma variedade de perspectivas e procedimentos. Podemos assumir que os stakeholders não carregam a responsabilidade, ainda que fosse desejável, de levar em consideração as pautas dos outros setores. Sendo assim, a sociedade civil organizada não desenvolve pautas sobre infraestrutura e padrões de IoT, bem como o setor privado, de desenvolvedores da tecnologia, não priorizam demandas por liberdade de expressão. No entanto, no que se refere ao desenvolvimento de políticas públicas, os diversos atores interessados, quais sejam, o setor privado, a sociedade civil organizada, o poder público e a comunidade técnica ou científica, devem ser ouvidos e postos em diálogo para o estabelecimento de consensos sobre qual será a melhor forma de desenvolvimento da tecnologia, ouvidas e sopesadas todas as demandas.

Quando se tratam de cidades inteligentes, acordos entre o setor privado - desenvolvedores de dispositivos, inteligências artificiais, conectividade e outras soluções tecnológicas - e o setor público podem ser relacionados ao câmbio de informações coletadas. Recentemente, a Prefeitura de São Paulo sofreu represália da sociedade civil ao informar que ofereceria os bancos de dados do Bilhete Único (DANTAS, D., DANTAS, T, 2017) como moeda nos programas de privatização (SETO, 2017) da cidade e que faria uso dos dados de navegação dos usuários do “Wi-Fi Livre” para lhes encaminhar propaganda direcionada (BIONI, 2017).

Ocorre que esse modelo de negócio é típico de uma administração que encaminha políticas públicas através do relacionamento estreito com o setor privado, não envolvendo a sociedade civil nas mesas de discussão, contribuindo para uma governança pouco transparente e participativa. Dessa forma, não é de se esperar que o setor público, sobretudo o de caráter privatista, priorize a garantia de direitos fundamentais em detrimento do fortalecimento do mercado. Dessa forma, ganha força a necessidade do envolvimento dos setores da sociedade civil organizada na construção e na tomada de decisões de impacto social. Como bem dito na Declaração

## da Sociedade Civil, no âmbito da Cúpula Mundial da Sociedade da Informação:

Decisões tecnológicas devem ser tomadas com o objetivo de ir ao encontro de necessidades vitais das pessoas e não com o fim de enriquecer empresas ou tornar possível o controle antidemocrático dos governos. Sendo assim, decisões fundamentais concernentes ao design e ao uso de tecnologias devem ser tomadas em cooperação com a sociedade civil, incluindo usuários finais, engenheiros e cientistas.” (...) “São as pessoas quem, inicialmente, formam e moldam a sociedade. E com a sociedade da informação e da comunicação não é diferente. Os atores da sociedade civil têm sido inovadores-chave e modeladores da tecnologia, da cultura e dos conteúdos da informação e da comunicação, e assim continuarão no futuro (CIVIL SOCIETY DECLARATION, 2003).

Naturalmente, leva-se a crer que a governança da IoT ou, mais delimitadamente, das cidades inteligentes, não deve ser discutida em separado da Internet como um todo. O desenvolvimento dessa tendência, de largo impacto no cotidiano coletivo, deve levar em consideração as técnicas e os valores da governança, como ocorre com a Internet. Um envolvimento limitado na construção de políticas, tal como nos casos ilustrativos de São Paulo, levará ao esvaziamento de direitos fundamentais. A privacidade deve ser levada em conta desde o desenho dos dispositivos até a construção de políticas públicas que tenham como eixo o uso dessas tecnologias. Em suma, o cidadão deve ser protegido através da busca constante de soluções que busquem preservar sua autonomia. A isso se deve uma abordagem multissetorial ao desenvolvimento e aplicação de tecnologias de largo impacto.

## 5 | CONCLUSÃO

Cidades inteligentes não são, necessariamente, cidades melhores. Para além de serem paradigmas da modernidade e do desenvolvimento, podem se tornar locais de panoptismo eletrônico, nas quais todos são constantemente observados .

Confiança e sustentabilidade são valores essenciais para o sucesso do desenvolvimento de tecnologias, principalmente aquelas que terão impacto global. A garantia de segurança e privacidade são desafios lançados ao universo de IoT e, quanto antes enfrentados, maior a probabilidade de uma integração amigável ao ecossistema de outros dispositivos e, sobretudo, de pessoas.

A regulação da tecnologia, impulsionando pautas tangentes à ética e à transparência, não limitando o processo inovador, mas pondo-o em conformidade com valores sociais e humanos, configura etapa primordial ao desenvolvimento da sociedade. A proteção de dados pessoais deve assumir a dianteira deste universo, visto caminharmos a um cenário pansensível, repleto de sensores e processamento de informações pessoais. Sendo assim, a manifestação da vontade e o consentimento devem estar nas bases do desenho de cidades inteligentes.

A boa governança, participativa, com a cooperação igualitária dos setores de interesse ao desenvolvimento da Internet, de roupagem multissetorial, parece ser o

caminho a ser percorrido, integrando as cidades inteligentes ao universo geral da Internet. Assim, o desenvolvimento de infraestruturas, a inovação, as políticas públicas e os padrões de segurança caminharão lado a lado com a garantia de direitos, promovendo uma experiência segura e inclusive na Internet e nas cidades.

## REFERÊNCIAS

ANDERSON, J; RAINIE, L. **The Internet of Things Will Thrive by 2025**. Pew Research Center: Internet & Technology, maio de 2014. Disponível em <http://www.pewinternet.org/2014/05/14/internet-of-things/>. Acesso em 31 de janeiro de 2018.

ASHTON, Kevin. **The “Internet of Things” Thing**. RFID Journal. J junho de 2009. Disponível em <http://www.rfidjournal.com/articles/view?4986>. Acesso em 31 de janeiro de 2018.

BANISAR, D; GUILLEMIN, G; BLANCO, M. **Proteção de Dados Pessoais no Brasil: Análise dos Projetos de Lei em Tramitação no Congresso Nacional**. Article 19. Novembro de 2016. Disponível em [https://docs.google.com/document/d/1d\\_j3IP5NUy-1LfUKr\\_ia6KT9o7mz9ntQYqjKLPP7zpo/edit](https://docs.google.com/document/d/1d_j3IP5NUy-1LfUKr_ia6KT9o7mz9ntQYqjKLPP7zpo/edit). Acesso em 31 de janeiro de 2018

BIONI, Bruno. **Expansão do Wi-Fi público às “custas” de dados pessoais: O caso de SP e a necessidade de avançar em políticas municipais de proteção dos dados pessoais**. 2017. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protacao-de-dados/expansao-do-wi-fi-publico-as-custas-de-dados-pessoais-17072017>. Acesso em 29 de janeiro de 2018.

BIONI, Bruno. **Xeque-Mate: O Tripé da Proteção de Dados Pessoais no Jogo de Xadrez das Iniciativas Legislativas no Brasil**. GPoPAI – Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. São Paulo: setembro de 2015.

CARAGLIU, A; NIJKAMP, P. **Smart cities in Europe**. 3rd Central European Conference in Regional Science – CERS, pág 45-59, 2009.

CISCO. **Case Study: City of Copenhagen**. CISCO Website. Disponível em <https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/copenhagen.html>. Acesso em 31 de janeiro de 2018

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4060/2012**. Disponível em [http://www.camara.gov.br/proposicoesWeb/prop\\_mostrarintegra%3Bjsessionid=760B5D6AD84435C695BF7614B6781D39.proposicoesWebExterno2?codteor=1001750&filename=PL+4060/2012](http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra%3Bjsessionid=760B5D6AD84435C695BF7614B6781D39.proposicoesWebExterno2?codteor=1001750&filename=PL+4060/2012). Acesso em 31 de janeiro de 2018

DANTAS, T; DANTAS, D. **Doria oferece dados de usuários do Bilhete Único à iniciativa privada**. In: O Globo. 2017. Disponível em: <<https://oglobo.globo.com/brasil/doria-oferece-dados-de-usuarios-do-bilhete-unico-iniciativa-privada-20942133#ixzz55oTMcwZd>>. Acesso em 30 de janeiro de 2018.

DATOO, Siraj. **This Recycling Bin is Following You**. Quartz. Agosto de 2013. Disponível em <https://qz.com/112873/this-recycling-bin-is-following-you/>. Acesso em 31 de janeiro de 2018.

DONEDA, Danilo. **A Proteção de Dados Pessoas Como um Direito Fundamental**. Espaço Jurídico. Joaçaba: 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Renovar, Rio de Janeiro, pág 1-410, 2006.

DONEDA, Danilo apud CONVERGÊNCIA DIGITAL. **Avanço Tecnológico Muda o Conceito de Dados Anônimos ou Sensíveis.** Convergência Digital. Setembro de 2016. Disponível em <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=43500&sid=4>. Acesso em 31 de janeiro de 2018.

EVANS, Dave. **The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.** In: Cisco Internet Business Solutions Group (IBSG). 2011. Disponível em: [https://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/loT\\_IBSG\\_0411FINAL.pdf](https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/loT_IBSG_0411FINAL.pdf). Acesso em 11 de janeiro de 2018.

Federal Trade Commission. **Internet of Things: Privacy and Security in a Connected World.** FTC Staff Report. Janeiro de 2015. Disponível em: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Acesso em 31 de janeiro de 2018.

FINCH, K; TENE, O. **Welcome to the Metropticon: Privacy in a Hyperconnected Town.** Fordham Urban Law Journal, nº 5, 1681-1615, abr. 2015.

FROLIC STUDIO. **IOT Design Manifesto.** Maio de 2015. Disponível em <https://www.iotmanifesto.com/wp-content/themes/Manifesto/Manifesto.pdf>. Acesso em 31 de janeiro de 2018.

FUSTER, G; SCHERRER, A. **Big Data and Smart Devices and Their Impact on Privacy.** European Parliament – Directorate General For Internet Policies. 2015. Disponível em [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL\\_STU\(2015\)536455\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf). Acesso em 31 de janeiro de 2018

GIFFINGER, R et al. **Smart cities: Ranking of European medium-sized cities.** Centre of Regional Science, Vienna: outubro de 2007

HERTSGAARD, Mark. **How the Pentagon Punished the NSA Whistleblowers.** The Guardian. Maio de 2016. Disponível em <https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers>. Acesso em 31 de janeiro de 2018.

IBM. **Smart Cities: New Cognitive Approaches to long-standing challenges.** IBM Website. Disponível em [https://www.ibm.com/smarterplanet/us/en/smarter\\_cities/overview/index.html](https://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/index.html). Acesso em 31 de janeiro de 2018.

JACOBS, Jane. **Morte e Vida de Grandes Cidades.** 3ª Ed. São Paulo: Martins Fontes, 2011, pág 64.

MARKETS AND MARKETS. **Smart Cities Market worth 1,201.69 Billion USD by 2022.** Markets and Markets Website. Disponível em <https://www.marketsandmarkets.com/PressReleases/smart-cities.asp>. Acesso em 31 de janeiro de 2018.

MURDOCK, Jason. **This is how China uses mass surveillance and big data to curb social unrest.** Business Insider. Abril de 2016. Disponível em <http://uk.businessinsider.com/china-uses-mass-surveillance-to-curb-unrest-2016-4?r=US&IR=T>. Acesso em 31 de janeiro de 2018.

NETMUNDIAL. **Declaração Multissetorial de São Paulo (NETmundial). Global Multistakeholder Meeting on the Future of Internet Governance.** Abril de 2014. Disponível em [https://www.cgi.br/media/docs/publicacoes/4/Documento\\_NETmundial\\_pt.pdf](https://www.cgi.br/media/docs/publicacoes/4/Documento_NETmundial_pt.pdf). Acesso em 31 de janeiro de 2018

PRIVACY INTERNATIONAL. **Case Study: Smart Cities and Our Brave New World.** Privacy International Website. Disponível em <https://privacyinternational.org/node/30>. Acesso em 31 de janeiro de 2018

PRIVACY INTERNATIONAL. **Smart Cities.** Privacy International Website. Disponível em <https://privacyinternational.org/topics/smart-cities>. Acesso em 31 de janeiro de 2018.

RE, C. et al. **Extracting Databases from Dark Data with DeepDive**. SIGMOD. São Francisco: Junho de 2016.

ROTHMAN, Joshua. **Takes: The N.S.A.'s Surveillance Programs**. New Yorker. Junho de 2013. Disponível em <https://www.newyorker.com/books/double-take/takes-the-n-s-a-s-surveillance-programs>. Acesso em 31 de janeiro de 2018

SCHNEIER, Bruce. **How we sold our souls – and more – to the giants. Schneier on Security**, 2015. Disponível em [https://www.schneier.com/essays/archives/2015/05/how\\_we\\_sold\\_our\\_soul.html](https://www.schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html). Acesso em 02/10/2017.

SETO, Guilherme. **'Pré-candidato', Doria vê privatizações de São Paulo como exemplo ao Brasil**. Folha de S. Paulo. Disponível em <http://www1.folha.uol.com.br/cotidiano/2017/10/1924386-pre-candidato-doria-ve-privatizacoes-de-sao-paulo-como-exemplo-ao-brasil.shtml>. Acesso em 30 de janeiro de 2018.

SIDEWALK LABS. **Sidewalk Labs is Reimagining Cities to Improve Quality of Life**. Sidewalk Labs Website. Disponível em <https://www.sidewalklabs.com/>. Acesso em 31 de janeiro de 2018.

SOLOVE, Daniel. **A Taxonomy of Privacy**. University of Pennsylvania Law Review. Janeiro de 2006. Disponível em [https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477\(2006\).pdf](https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf). Acesso em 31 de janeiro de 2018.

WATTS, J; PURNELL, N. **Singapore Is Taking the 'Smart City' to a Whole New Level**. The Wall Street Journal. Abril de 2014. Disponível em <https://www.wsj.com/articles/singapore-is-taking-the-smart-city-to-a-whole-new-level-1461550026>. Acesso em 31 de janeiro de 2018

WEISER, Mark. **The Computer for the 21st Century**. ACM SIGMOBILE Mobile Computing and Communications Review - Special issue dedicated to Mark Weiser, New York, Volume 3, 1999. Disponível em: <http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>. Acesso em 31 de janeiro de 2018.

WESTIN, Alan. **Privacy and Freedom**. Washington and Lee Law Review. Janeiro de 1968. Disponível em <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/>. Acesso em 31 de janeiro de 2018.

WORKING GROUP ON INTERNET GOVERNANCE. **Report of the Working Group on Internet Governance**. Junho de 20. Disponível em <http://www.wgig.org/docs/WGIGREPORT.pdf>. Acesso em 31 de janeiro de 2018

WSIS Civil Society Plenary. **"Shaping Information Societies for Human Needs": Civil Society Declaration to the World Summit on the Information Society**. 2003. Disponível em <https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf>. Acesso em 30 de janeiro de 2018.

ZANATTA, Rafael. **Internet das Coisas: Privacidade e Segurança na Perspectiva dos Consumidores**. IDEC. 2017. Disponível em [https://www.idec.org.br/ckfinder/userfiles/files/Contribuic%CC%A7a%CC%83o%20Pu%CC%81blica\\_%20Idec\\_%2006022017.pdf](https://www.idec.org.br/ckfinder/userfiles/files/Contribuic%CC%A7a%CC%83o%20Pu%CC%81blica_%20Idec_%2006022017.pdf). Acesso em 31 de janeiro de 2018

ZUBOFF, Shoshana. Big Other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, nº 30, Cambridge, abr. 2015.

## **SOBRE O ORGANIZADOR**

**ERNANE ROSA MARTINS** Doutorado em andamento em Ciência da Informação com ênfase em Sistemas, Tecnologias e Gestão da Informação, na Universidade Fernando Pessoa, em Porto/Portugal. Mestre em Engenharia de Produção e Sistemas, possui Pós-Graduação em Tecnologia em Gestão da Informação, Graduação em Ciência da Computação e Graduação em Sistemas de Informação. Professor de Informática no Instituto Federal de Educação, Ciência e Tecnologia de Goiás - IFG (Câmpus Luziânia), ministrando disciplinas nas áreas de Engenharia de Software, Desenvolvimento de Sistemas, Linguagens de Programação, Banco de Dados e Gestão em Tecnologia da Informação. Pesquisador do Núcleo de Inovação, Tecnologia e Educação (NITE), certificado pelo IFG no CNPq.

Agência Brasileira do ISBN  
ISBN 978-85-7247-390-3

