

**UNIVERSIDADE FEDERAL DE SERGIPE**  
**PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO**  
**MESTRADO EM ADMINISTRAÇÃO**

**CARLOS CESAR SANTOS**

**ASPECTOS DETERMINANTES PARA O FORNECIMENTO DE INFORMAÇÕES  
PESSOAIS EM AMBIENTES INTELIGENTES**

**SÃO CRISTÓVÃO**  
**Fevereiro/2016**

**CARLOS CESAR SANTOS**

**ASPECTOS DETERMINANTES PARA O FORNECIMENTO DE INFORMAÇÕES  
PESSOAIS EM AMBIENTES INTELIGENTES**

Dissertação apresentada como requisito parcial para obtenção do título de mestre em administração pelo programa de pós-graduação em administração da Universidade Federal de Sergipe, Campus de São Cristóvão, Sergipe.

**Orientador: Prof. Dr. Jefferson David  
Araújo Sales**

**SÃO CRISTÓVÃO  
Fevereiro/2016**

*“As crianças que pensam em um amanhã diferente, para que elas tenham a oportunidade de construir um amanhã mais humano e conectado.”*

## **AGRADECIMENTOS**

Agradeço a todos os 228 parceiros anônimos espalhados pelo Brasil, não sei onde estão e nem quem são, mas sem a atenção e o tempo que vocês dedicaram nenhum resultado teria sido encontrado e nada disso teria sido possível. Obrigado usuários respondentes da pesquisa.

Obrigado amigos pesquisadores, agradeço a todos de Alves (1999) a Zorzi (2010), que mesmo a distância contribuíram para construção dessa pesquisa, a luz dos trabalhos de vocês foi possível ir além. Cada citação feita foi mais do que o cumprimento de uma norma acadêmica, compreendam este citar como uma sincera homenagem ao reconhecimento da qualidade do trabalho de vocês.

A todos que compõem o PROPADM, meus sinceros agradecimentos, das aulas de cada docente que tive a oportunidade de participar, as dicas relâmpagos da professora Maria Elena nos corredores e na secretaria. Ao secretário e parceiro Eduardo Bomfim e sua paciência em esperar eu sair da sala de pesquisa quase todos os dias dos últimos meses, mesmo estando em seu horário de saída. A Capes pela bolsa de estudos concedida, sem a qual eu não teria chegado até o fim. E aos alunos desconhecidos da minha turma, por rapidamente terem sido promovidos a amigos, a luta de cada um de nós, rapidamente se tornou a luta de todos nós.

Um agradecimento mais que especial ao “dá para melhora isso”, Jefferson meu muito obrigado por ir além, ir além da orientação acadêmica e me orientar no crescimento como profissional e como pessoa. Cada dica, ensinamento e principalmente seu exemplo como profissional e como pessoa serão lembrados e levados para a vida porque transcendem a relação entre orientador e orientando, nos torna amigos.

Obrigado família, sejam os de sangue ou os de espírito, aos presentes e aos ausentes dessa jornada, aos que contribuíram com palavras e aos que contribuíram com silêncio. E de forma mais que especial, meu muito obrigado a guerreira que é e será sempre meu exemplo, que desde pequeno repete aos meus ouvidos os ensinamentos de quem sabe mais do que nós, “o conhecimento é a única riqueza que ninguém jamais tirará de você”, mãe meu muito obrigado.

*“A ciência de hoje é a tecnologia de amanhã”.*

(Edward Teller)

## RESUMO

Na última década a internet tornou-se uma ferramenta presente no cotidiano das pessoas e das organizações e por vez indispensável ao bom funcionamento dos negócios. Com o crescente incremento das infraestruturas de redes e popularização em massa da rede de alta velocidade, emerge um avanço relacionado à utilização da internet tornando-a uma plataforma global para deixar máquinas e objetos inteligentes capazes de comunicarem-se de forma autônoma. Esta possibilidade permite que conteúdos e serviços estejam em torno das pessoas, sempre disponíveis, facilitando a comunicação e abrindo o caminho para novas aplicações, possibilitando novas formas de trabalho, de interação e de entretenimento, fazendo com que um novo padrão de vida e de trabalho seja desenvolvido. Este novo padrão torna-se possível através dos avanços das Tecnologias da Informação e Comunicação - TIC's até uma nova concepção definida como *Internet of Things* - IoT. Entretanto, com uma variada coleta de dados e informações, para variados fins, no cotidiano das pessoas e das organizações, a coleta autônoma dos dados e das informações torna a privacidade um dos principais desafios em relação à IoT. Neste contexto, esta pesquisa objetivou investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Coisas ao fornecerem informações pessoais em ambientes inteligentes. A pesquisa caracterizou-se como positivista, de natureza quantitativa, do tipo exploratória e descritiva, sua implementação aconteceu por meio da estratégia de pesquisa de campo, tendo como instrumento de coleta de dados um questionário autoaplicável, que foi disponibilizado para respondentes em território brasileiro. Adotou-se na análise dos dados coletados uma linha quantitativa baseada em técnicas estatísticas, em que buscou-se cruzar os dados a fim de alcançar o objetivo da pesquisa. Dentre as principais conclusões decorrentes da pesquisa, intuiu-se que o ambiente de uso se configura como um aspecto determinante ao fornecimento de informação ao ambiente inteligente de maior influência entre os outros aspectos encontrados. Foi percebido que os usuários tendem a dedicar considerável atenção a segurança e a privacidade das informações que possuem, disponibilizando-as com ressalvas e cuidados. Contudo por vezes, transferem a responsabilidade pela segurança das informações para terceiros, buscando reduzir ao máximo o número de critérios a serem analisados antes de tomar a decisão de disponibilizar seus dados.

**Palavras-chaves:** Internet das Coisas; Privacidade; Ambiente Inteligente

## ABSTRACT

In the last decade the internet has become a tool present in the daily lives of people and organizations and time essential to the smooth operation of businesses. With the increasing development of infrastructure networks and popularization mass of high-speed network, emerges a related Internet use advance making it a global platform to make intelligent machines and objects able to communicate up autonomously. This possibility enables content and services are around people, always available, facilitating communication and paving the way for new applications, enabling new forms of work, interaction and entertainment, making a new pattern of living and working is developed. This new standard is made possible through advances in Information and Communication Technologies - ICTs to a new design set to Internet of Things - IoT. However, with a varied collection of data and information for various purposes, in the daily lives of people and organizations, autonomous data collection and information makes privacy a major challenge regarding the IoT. In this context, this study aimed to investigate the aspects that determine the action of Internet technology users of Things to supply personal information in intelligent environments. The research was characterized as positivist, quantitative, exploratory and descriptive, its implementation took place through field research strategy, with the data collection instrument a self-administered questionnaire, which was available to respondents in Brazil. It was adopted in the analysis of data collected quantitative line based on statistical techniques, in which we attempted to cross the data in order to achieve the objective of the research. Among the main conclusions from the research, it intuited that the use of environment is a determining aspect to providing information to the intelligent environment of greater influence among other aspects found. It was noticed that users tend to devote considerable attention to security and privacy of information we have, providing them with qualifications and care. However sometimes transfer responsibility for security of the information to third parties seeking to reduce the maximum number of criteria to be considered before making the decision to make available their data.

**Keywords:** Internet of Things; Privacy; intelligent environment

## LISTA DE FIGURAS

FIGURA 1: DIAGRAMA CONCEITUAL DA PESQUISA .....	21
FIGURA 2: VISÕES DA INTERNET DAS COISAS.....	24
FIGURA 3: A IOT NAS TAREFAS DIÁRIAS.....	30
FIGURA 4: DESENHO DA PESQUISA .....	57
FIGURA 5: VOLUME DE INFORMAÇÃO CONSENTIDA.....	81
FIGURA 6: ASPECTOS DETERMINANTES PARA O FORNECIMENTO DE DADOS E INFORMAÇÕES EM AMBIENTES INTELIGENTES.....	87

## LISTA DE QUADROS

QUADRO 1: INTERNET DAS COISAS .....	22
QUADRO 2: LINHAS DE FRONTEIRAS PESSOAIS .....	39
QUADRO 3: PRINCÍPIOS FUNDAMENTAIS DA PRIVACIDADE.....	41
QUADRO 4: QUADRO DE CONSISTÊNCIA DO INSTRUMENTO DE COLETA DE DADOS .....	56
QUADRO 6: PERFIL DOS USUÁRIOS RESPONDENTES DA PESQUISA .....	65
QUADRO 7: TIPOS DE TECNOLOGIAS INTELIGENTES.....	68
QUADRO 8: AMBIENTE DE USO E PRINCIPAIS FINALIDADES.....	72
QUADRO 9: DADOS E INFORMAÇÕES DISPONIBILIZADOS POR MEIO DOS DISPOSITIVOS .....	76
QUADRO 10: ASPECTOS DETERMINANTES PARA O FORNECIMENTO DE DADOS E INFORMAÇÕES.....	83
QUADRO 11: RESULTADOS PREDOMINANTES ENCONTRADOS EM CAMPO .....	84

## LISTA DE GRÁFICOS

<b>GRÁFICO 1: GÊNERO DOS RESPONDENTES.....</b>	<b>61</b>
<b>GRÁFICO 2: FAIXA ETÁRIA.....</b>	<b>62</b>
<b>GRÁFICO 3: DISTRIBUIÇÃO REGIONAL DA AMOSTRA .....</b>	<b>63</b>
<b>GRÁFICO 4: GRAU DE ESCOLARIDADE DOS RESPONDENTES.....</b>	<b>64</b>
<b>GRÁFICO 5: DISPOSITIVOS INTELIGENTES .....</b>	<b>66</b>
<b>GRÁFICO 6: USO DIÁRIO DE DISPOSITIVOS INTELIGENTES.....</b>	<b>67</b>
<b>GRÁFICO 7: DISPOSITIVOS EM DESUSO.....</b>	<b>67</b>
<b>GRÁFICO 8: AMBIENTES DE USO.....</b>	<b>69</b>
<b>GRÁFICO 9: AMBIENTES DE USO EVITADOS .....</b>	<b>70</b>
<b>GRÁFICO 10: FINALIDADES DE USO DOS DISPOSITIVOS.....</b>	<b>70</b>
<b>GRÁFICO 11: FINALIDADES DE USO EVITADAS PELOS USUÁRIOS .....</b>	<b>71</b>
<b>GRÁFICO 12: TRÊS PRINCIPAIS FINALIDADES DE USO DOS DISPOSITIVOS .....</b>	<b>72</b>
<b>GRÁFICO 13: DADOS E INFORMAÇÕES DISPONIBILIZADOS .....</b>	<b>73</b>
<b>GRÁFICO 14: DADOS E INFORMAÇÕES QUE EVITASSE DISPONIBILIZAR.....</b>	<b>74</b>
<b>GRÁFICO 15: DADOS E INFORMAÇÕES DISPONIBILIZADOS EM USO DOMÉSTICO ..</b>	<b>75</b>
<b>GRÁFICO 16: DADOS E INFORMAÇÕES .....</b>	<b>75</b>
<b>DISPONIBILIZADOS EM USO PROFISSIONAL .....</b>	<b>75</b>
<b>GRÁFICO 17: ASPECTOS DETERMINANTES PARA O FORNECIMENTO DE DADOS E INFORMAÇÕES EM AMBIENTE DOMÉSTICO.....</b>	<b>77</b>
<b>GRÁFICO 18: CONDIÇÕES QUE DETERMINAM O FORNECIMENTO DE INFORMAÇÕES PARA USUÁRIOS DO GÊNERO MASCULINO.....</b>	<b>79</b>
<b>GRÁFICO 19: CONDIÇÕES QUE DETERMINAM O FORNECIMENTO DE INFORMAÇÕES PARA USUÁRIOS DO GÊNERO FEMININO.....</b>	<b>79</b>
<b>GRÁFICO 20: CONDIÇÕES PRINCIPAIS PARA O FORNECIMENTO DE INFORMAÇÕES .....</b>	<b>80</b>
<b>GRÁFICO 21: TIPOS DE INFORMAÇÕES QUE SÃO FORNECIDAS NO AMBIENTE INTELIGENTE X CONDIÇÃO DE FACILIDADE DE USO DO DISPOSITIVO INTELIGENTE .....</b>	<b>81</b>
<b>GRÁFICO 22: ASPECTOS DETERMINANTES PARA O FORNECIMENTO DE DADOS E INFORMAÇÕES EM AMBIENTE PROFISSIONAL .....</b>	<b>82</b>

## SUMÁRIO

<b>1. INTRODUÇÃO</b> .....	<b>13</b>
1. 2 <i>Situação Problemática</i> .....	16
1. 3 <i>Objetivos</i> .....	17
1. 3. 1 <i>Objetivo Geral</i> .....	17
1. 3. 2 <i>Objetivos Específicos</i> .....	17
1.4 <i>Justificativa</i> .....	18
<b>2. FUNDAMENTAÇÃO TEÓRICA</b> .....	<b>21</b>
2. 1 <i>Origem da Internet das Coisas</i> .....	21
2. 1.1 <i>Evolução dos padrões em TIC</i> .....	22
2. 1. 2 <i>Internet das Coisas como novo posicionamento tecnológico</i> .....	26
2. 2 <i>O ambiente inteligente da Internet das Coisas</i> .....	28
2. 2. 1 <i>A IoT no ambiente doméstico</i> .....	28
2. 2. 2 <i>Negócios inteligentes</i> .....	32
2. 3 <i>Privacidade e a IoT</i> .....	37
2. 3. 1 <i>Privacidade na era da informação</i> .....	38
2. 3. 2 <i>Perspectiva legal da privacidade de informação</i> .....	42
<b>3. PROCEDIMENTOS METODOLÓGICOS</b> .....	<b>48</b>
3. 1 <i>Posicionamento Epistemológico da Pesquisa</i> .....	48
3. 2 <i>Caracterização da Pesquisa</i> .....	50
3. 3 <i>Método de Pesquisa</i> .....	51
3. 4 <i>Estratégia da Pesquisa</i> .....	52
3. 4. 1 <i>Universo e Público Alvo</i> .....	52
3. 4. 2 <i>Amostra</i> .....	53
3. 5 <i>Coleta dos Dados</i> .....	55
3. 5. 1 <i>Desenho da Pesquisa</i> .....	56
3. 6 <i>Tratamento dos Dados</i> .....	58
3. 8 <i>Cuidados Metodológicos</i> .....	59
<b>4 ANÁLISE DOS DADOS</b> .....	<b>61</b>
4.1 <i>Perfil dos respondentes</i> .....	61
4.2 <i>Tipos de tecnologias inteligentes</i> .....	65
4.3 <i>Ambiente de uso dos dispositivos e principais finalidades</i> .....	69
4.4 <i>Dados e informações disponibilizados por meio dos dispositivos</i> .....	73
4.5 <i>Aspectos determinantes para o fornecimento de dados e informações</i> .....	77
4.5 <i>Resultados predominantes achados em campo</i> .....	83
<b>5 CONCLUSÕES</b> .....	<b>89</b>
5.1 <i>Limitações do Estudo</i> .....	91
5.2 <i>Indicações para Futuras Pesquisas</i> .....	92
<b>REFERÊNCIAS BIBLIOGRÁFICAS</b> .....	<b>93</b>
<b>APÊNDICE A: INSTRUMENTO DE COLETA DE DADOS</b> .....	<b>99</b>

*“A primeira regra de qualquer tecnologia utilizada nos negócios é que a automação aplicada a uma operação eficiente aumentará a eficiência. A segunda é que a automação aplicada a uma operação ineficiente aumentará a ineficiência”*

(Bill Gates)

## 1. INTRODUÇÃO

Cerca de três bilhões de pessoas ao redor do mundo usam a Internet para se comunicar, navegar na Web, acessar conteúdos e serviços multimídia, jogos, interagir em redes sociais e muitas outras aplicações (ONU, 2015). Com o crescente incremento das infraestruturas de redes e popularização em massa da internet de alta velocidade, emerge um avanço relacionado à utilização da internet tornando-a uma plataforma global para deixar máquinas e objetos inteligentes capazes de comunicarem-se de forma autônoma (MIORANDI et al., 2012).

Gao e Bai (2014) destacam que durante a próxima década, a rede inter-existirá como um tecido sem costura de redes clássicas e objetos ligados em rede. O conteúdo e serviços estarão em torno das pessoas, sempre disponível, facilitando a comunicação e abrindo o caminho para novas aplicações, possibilitando novas formas de trabalho, de interação, de entretenimento, fazendo com que um novo padrão de vida seja desenvolvido. Este novo padrão de vida, torna-se possível através dos avanços das Tecnologias da Informação e da Comunicação - TIC's até uma nova concepção definida como *Internet of Things* - IoT.

O termo *Internet of Things* foi cunhado pela primeira vez, em 1999 por Ashton, um dos pioneiros da tecnologia britânica que ajudou a desenvolver o conceito (GUBBI et al., 2013). A IoT visa estender os benefícios da internet proporcionando uma conectividade constante, desenvolvendo uma capacidade de controle remoto e compartilhamento de dados para os bens no mundo físico (PEOPLES et al., 2013).

A Internet das Coisas - IoT advém do conceito de presença generalizada em torno das pessoas e de uma variedade de coisas ou objetos, através de *Radio Frequency IDentification* - RFID<sup>1</sup>, sensores, atuadores, *gadget*<sup>2</sup> como *smartphones*, *tablet*, televisores, pulseiras e relógios inteligentes, etc., por meio de esquemas de endereçamento exclusivos que são capazes de interagir uns com os outros e cooperar com os seus vizinhos para alcançar objetivos comuns (ATZORI; IERA; MORABITO, 2010).

---

<sup>1</sup> Identificação por radiofrequência

<sup>2</sup> Dispositivos eletrônicos portáteis de função prática e específica

Dentro dessa perspectiva, o termo *Internet of Things* - IoT é amplamente usado para se referir a ambos: A rede global resultante da interligação dos objetos inteligentes; ao conjunto de tecnologias de apoio necessárias para concretizar essa visão; e ao conjunto de aplicações e serviços que alavancam tais tecnologias para abrir novas oportunidades de negócios e de mercados (MIORANDI et al., 2012).

A eficácia da IoT reside no alto impacto que ela se dispõe a proporcionar sobre diversos aspectos da vida cotidiana e do comportamento de usuários potenciais (PEOPLES et al., 2013). Do ponto de vista de um usuário privado, os efeitos mais evidentes da introdução da IoT estão em suas funções assistidas, como em cuidados com a saúde, orientação de aprendizagem e controle doméstico, sendo estes apenas alguns exemplos dos campos de aplicação da IoT. Da mesma forma, a partir da perspectiva dos usuários de negócios, as consequências mais aparentes serão igualmente visíveis em áreas como automação e manufatura industrial, logística, processo de gestão e tomada de decisão, transporte inteligente de pessoas e bens (ATZORI; IERA; MORABITO, 2010).

Com uma variada coleta de dados e informações, para variados fins, no cotidiano das pessoas, seja em ambientes domésticos de usuários privados ou em ambientes profissionais de usuários de negócios, a coleta autônoma dos dados e das informações dos usuários torna a privacidade uma das principais preocupações éticas com relação à Internet das Coisas. Entendida por Chabridon et al. (2014) como uma questão crucial que pode limitar a implantação da visão IoT seja para usuários privados ou para organizações.

Chabridon et al. (2014) e Weber e Weber (2010) ressaltam que a privacidade é fundamental para o controle deste novo ambiente complexo. A troca de dados invisível e constante entre as coisas e as pessoas, e entre as coisas e outras coisas, irá ocorrer de forma que os proprietários e criadores desses dados não sejam identificados. A própria escala e capacidade das novas tecnologias vai ampliar este problema.

O termo privacidade transmite um grande número de conceitos e ideias. Comumente associa-se privacidade com a noção de um indivíduo que controla o acesso a sua informação pessoal. Weber e Weber (2010) identificam três áreas relacionadas com a privacidade, sendo elas: O espaço físico, que pode ser compreendido como um escudo contra objetos indesejados ou sinais; o poder de

tomada de decisão em relação ao fluxo de informações com o objetivo de proteger a liberdade de uma pessoa ao fazer escolhas a respeito de seus dados; e o controle de um indivíduo sobre o processamento da informação compreendendo a aquisição, divulgação e uso de informações pessoais.

No entanto, Chabrindon et al. (2014) afirmam que preservar a privacidade através do isolamento não é mais uma opção no mundo da informação e da comunicação de hoje. Para um contexto de ambiente inteligente gerado pela Internet das Coisas, onde as aplicações tornam-se de fácil usabilidade e as informações são disponibilizadas de maneira muitas vezes imperceptíveis, a privacidade é geralmente percebida pelos usuários como uma expectativa de estar em um estado de proteção sem ter que o perseguir ativamente.

Nessa linha, Marx e Murky (2001) identificaram quatro níveis de privacidade percebíveis pelas pessoas, estes níveis são posteriormente destacados por Chabrindon et al. (2014) para explicar a maneira como as pessoas percebem as violações a sua privacidade, definindo-os como fronteiras, sendo elas: A fronteira natural, caracterizada por impedir que a presença (ou sentimentos e/ou emoções) do indivíduo seja percebida através de um dos sentidos humanos, a exemplo do que proporciona as paredes, portas, cartas seladas, telefone e e-mail que criam fronteiras naturais a observação; a fronteira da sociedade, que envolve expectativas das pessoas para certos papéis sociais de profissionais (médicos, membros do clero, advogados) que não vão divulgar informações confidenciais; a fronteira espacial ou temporal, que separa a informação dos vários períodos ou aspectos da vida da pessoa; e a fronteira dos efeitos efêmeros ou transitórios, distinguidas pela ideia de que a interação e comunicação são esquecidas em breve.

Dentro dessa perspectiva de privacidade apresentada por Marx e Murky (2001) voltando-se aos recentes desafios da Internet das Coisas, esta pesquisa buscou aprimorar o entendimento das ações das pessoas em ambientes inteligentes, a fim de fornecer contribuições a teoria que se volta ao tema e a adoção desse tipo de tecnologia por organizações públicas e privadas, assim como o aperfeiçoamento dessas tecnologias por parte de desenvolvedores e fornecedores de serviços por esta possibilitados.

Em um contexto onde a Internet das Coisas apresenta-se como um fenômeno global, em franco desenvolvimento e que faz parte do cotidiano das

pessoas em diferentes escalas, esta pesquisa busca compreender de forma mais abrangente este fenômeno no Brasil, que a exemplo de outros países, também vem desenvolvendo iniciativas para regulamentar ações que viabilizem o desenvolvimento dessas tecnologias, como a Lei nº 12.965, de 23 de abril de 2014, que passa a regulamentar a internet no Brasil (PAMPLONA FILHO, 2014), definindo questões centrais para a privacidade dos usuários tais como a inviolabilidade do sigilo de suas comunicações, a garantia de privacidade de informações pessoais e o não monitoramento do usuário sem prévio consentimento.

Os números do panorama nacional que se apresentam favoráveis a implantação deste tipo de tecnologia, indicam que o número de *smartphones* em uso no país já supera o de computadores tradicionais e que a população brasileira já possui aproximadamente 306 milhões de dispositivos conectáveis a internet, isto é, 3 dispositivos para cada 2 habitantes (MEIRELLES, 2014).

Buscando explorar esta conjuntura favorável e em expansão, esta pesquisa realizou uma investigação focada nas pessoas que utilizam esse tipo de tecnologia dentro do território brasileiro, a fim de responder ao problema de pesquisa e cumprir os objetivos geral e específicos definidos neste estudo.

## 1. 2 Situação Problemática

Diante do cenário apresentado em que a privacidade se constitui como desafio constante para quaisquer envolvidos com o fenômeno da Internet das Coisas, sejam pessoas, organizações públicas ou privadas, desenvolvedores e fornecedores de soluções, o fornecimento de informações por parte das pessoas que compõem essa relação pessoas-coisas torna-se fundamental para a exploração plena do potencial da Internet das Coisas.

Contudo, até aqui foram identificadas diversas pesquisas que, ao destacarem o problema da privacidade na Internet das Coisas, o fazem por meio da ótica de sistemas de informação, investimentos em estruturas físicas e das tecnologias de segurança disponíveis (ATZORI; IERA; GIACOMO, 2010; EURICH; OERTEL; BOUTELLIER, 2010; MIORANDI et al., 2012; PEOPLES et al., 2013; GUBBI et al., 2013; CHABRINDON et al., 2014; DUTTON, 2014), e sem direcionar, ao menos

em princípio, o foco para as pessoas e os fatores por elas percebidos como relevantes ao fornecerem suas informações por meio destas tecnologias.

A relevância das pessoas nas transformações que a implementação de tecnologias baseadas na IoT podem promover e a necessidade de compreender os fatores que estas pessoas percebem como relevantes para fornecerem dados e informações por meio destas tecnologias é de fundamental importância para o direcionamento de políticas, investimentos e decisões seja na área pública ou privada, diante do exposto esta pesquisa buscou responder a seguinte pergunta: **Quais aspectos determinam a ação dos usuários ao fornecerem informações pessoais em ambientes inteligentes?**

### 1. 3 Objetivos

Esta subseção apresenta os objetivos geral e específicos da pesquisa, definidos a fim de orientar o curso das ações que a compõem, com o intuito de responder à questão de pesquisa.

#### 1. 3. 1 Objetivo Geral

Investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Cosias ao fornecerem informações pessoais em ambientes inteligentes.

#### 1. 3. 2 Objetivos Específicos

- Identificar os tipos de tecnologias inteligentes utilizadas pelas pessoas;
- Descrever as formas de uso cotidianas das tecnologias inteligentes;
- Identificar os tipos de dados e informações fornecidos em ambientes inteligentes;
- Analisar os aspectos determinantes para o fornecimento de dados e informações no ambiente inteligente.

#### 1.4 Justificativa

Por ter o potencial de prover mudanças em várias áreas da sociedade autores como Gao e Bai (2014), Miorandi et al. (2012), Chabrindon et al. (2014), Domingo (2012) e Weber e Weber (2010) defende que a Internet das Coisas requer inovações que vão além do foco da tecnologia industrial, exigindo também inovações sociais e organizacionais.

Dentre variadas preocupações relacionadas a IoT encontra-se o controle da privacidade, aspecto destacado por autores como Atzori, Iera e Giacomo (2010), Eurich, Oertel e Boutellier (2010), Miorandi et al. (2012), Domingo (2012), Peoples et al. (2013), Gubbi et al. (2013), Dutton (2014) e Chabrindon et al. (2014) ao afirmarem que tal desafio necessita de inovações apuradas em torno da privacidade do usuário, como o amparo da proteção de dados, dos direitos dos usuários e proteção intelectual. Desta forma, a pesquisa, ganha relevância por contribuir para a compreensão deste fenômeno com um olhar voltado para os usuários, contribuindo com o entendimento dos fatores que, para os usuários, possuem relevância nessa relação de importância da privacidade em detrimento do fornecimento de dados e informações.

Por seu turno, a privacidade dos dados e das informações para as organizações públicas, privadas e do terceiro setor remetem não apenas ao controle sobre as informações pessoais, mas também a propriedade intelectual, ao controle de investimentos, a pesquisas científicas e de mercado, ao planejamento e tomada de decisão, informações sigilosas pelas quais as organizações realizam investimentos para que estas permaneçam seguras (ATZORI; IERA; MORABITO, 2010). Contudo, um dos fatores que mais tornam vulneráveis as informações não são as estruturas de *software* e de *hardware*, mas as pessoas (CHABRINDON et al., 2014). Deste modo, os achados desta pesquisa contribuem para que as organizações adquiram uma perspectiva do fator humano na relação da privacidade da informação, identificando o que é compreendido pelo usuário como aspecto determinante para disponibilizarem informações, possibilitando evitar e sanar possíveis falhas em seus processos que venham por em risco suas informações.

As pesquisas na área de sistemas de informação produzem constantemente inovações focadas em aumentar a segurança da informação e a privacidade do usuário (CHABRINDON et al., 2014). No entanto, o distanciamento

entre os produtores dessas inovações e os usuários, abrem uma lacuna entre o que os profissionais da área de TI priorizam e o que é fator determinante para o usuário (WEBER; WEBER, 2010), neste aspecto, a pesquisa buscou oferecer subsídio capaz de aproximar estas realidades, identificando o que é determinante para o usuário em detrimento do que lhe é disponibilizado, suprimindo a lacuna da teoria presente nas atuais pesquisas sobre o tema.

No espectro da gestão, os resultados desta pesquisa poderão contribuir com um enfoque diferenciado que descentraliza a tomada de decisão por parte dos gestores, principalmente na área de gestão de sistema de informação (DUTTON, 2014), redirecionando a decisão de investimentos e de escolhas estratégicas da estrutura de TI das organizações, direcionadas a gestores e técnicos, e posicionando os usuários finais como parte importante, detentores das informações que buscam ser protegidas em sistemas complexos de garantias de privacidade.

Desta maneira, essa pesquisa almejou contribuir com perspectivas ainda não exploradas no campo das ciências da administração e de sistema de informação, no que se diz respeito a Internet das Coisas, preenchendo lacunas na literatura existente e propondo meios de melhor implementá-la numa realidade brasileira. Para alcançar tais pretensões, como apresentado na seção a seguir, pautou-se em um apanhado teórico fundamentado em estudos que se direcionam a temática aqui discutida, a fim de situar teoricamente a pesquisa e embasar os argumentos nela apresentados.

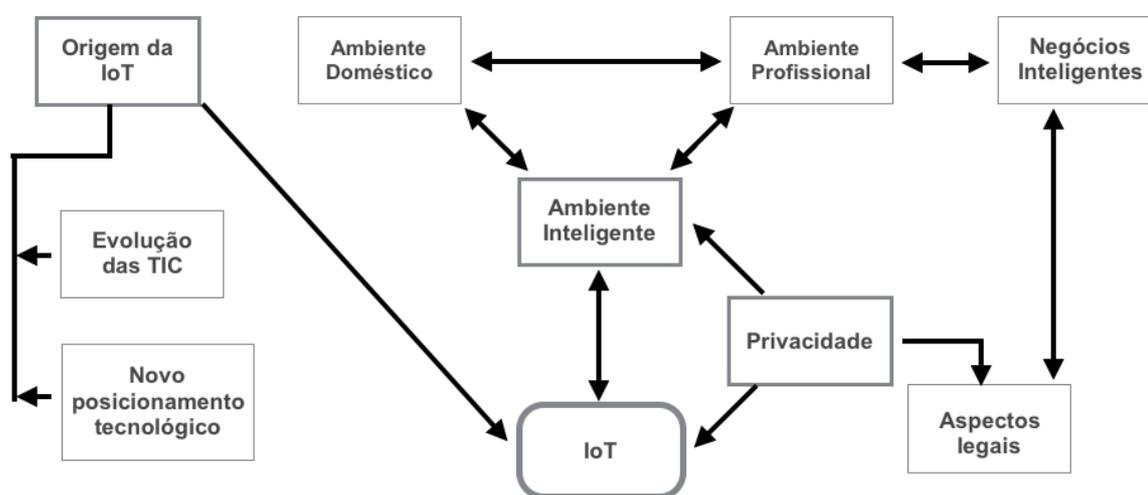
*“Esta tecnologia vai reinventar os negócios,  
mas as relações humanas continuarão a  
serem a chave para o sucesso”.*

(Stephen Covey)

## 2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresentará um apanhado teórico a respeito da temática em discussão, abordando aspectos elementares da Internet das Coisas e da privacidade buscando construir uma relação entre os elementos da pesquisa. Para melhor visualizar as ligações presentes entre as temáticas teóricas em discussão apresentase na figura 1, o diagrama conceitual da pesquisa.

**Figura 1: Diagrama Conceitual da Pesquisa**



Fonte: Elaborado pelo autor (2016).

Conforme o diagrama da figura 1 apresenta, a Internet das Coisa - IoT, é o elemento para o qual os conceitos e temáticas da pesquisa se unem, vislumbrando o resultado da evolução das TIC's como a origem da IoT, a possibilidade de novos negócios e a preocupação com a privacidade e seus aspectos legais que impactam diretamente nos negócios existentes e vindouros. É com o intuito de fundamentar teoricamente esta pretensa pesquisa que se segue as seções seguintes.

### 2. 1 Origem da Internet das Coisas

Desde quando foi criada até os dias atuais, as aplicações baseadas na internet passaram por uma série de mudanças até chegar ao fenômeno denominado Internet das Coisas. Compreender as diferenças entre aplicações que fazem uso dos recursos tradicionais da internet e o conjunto ferramental que compõem a IoT torna-

se essencial para a compreensão do fenômeno a ser estudado, suas principais aplicações potenciais e as que já estão em uso. As próximas seções que se seguem, tem como objetivo situar e contextualizar os aspectos que caracterizam a Internet das Coisas, suas origens, visões teóricas, campos de aplicação e dificuldades encontradas para a sua implementação.

### 2. 1.1 Evolução dos padrões em TIC

Ao longo de seus primeiros 40 anos, a internet tem sido usada principalmente para conectar pessoas através de troca de *e-mails*, fóruns de discussão e, cada vez mais, por meio de sites de redes sociais virtuais que coletam e distribuem dados e informações. Também nota-se que na atualidade a internet é utilizada para conectar dispositivos, máquinas e outros objetos, através de redes com e sem fio, criando um novo posicionamento tecnológico nomeado de *Internet of Things* (DUTTON, 2014).

A *Internet of Things* ou Internet das Coisas, como é chamada em português, ganhou uso pela primeira vez em 1999 por Ashton (2009), um dos autores pioneiros nesse tipo de tecnologia, cuja as pesquisas ajudaram a desenvolver o conceito atual desse posicionamento tecnológico. Contudo, é pertinente destacar que a aplicação e sofisticação deste conjunto emergente de tecnologias são suficientes para vê-lo como uma inovação genuína de aplicação da TIC's e da utilização da Internet (GUBBI, 2013).

**Quadro 1: Internet das Coisas**

IoT				
Ampliação	Ação	Meios	Finalidades	Possibilidades
<b>Da capacidade de conectividade constante</b>	Detecção	<i>Radio Frequency Identification</i> - RFID	Detecção ou acionamento de outros dispositivos que estão on-line	Armazenamento de informações
<b>Do compartilhamento de dados</b>	Marcação	Sensores e atuadores	Monitoramento	Envio de dados e informações
<b>Do controle a distância</b>	Identificação	Códigos de resposta rápida - QR	Identificação	Recebimento de de dados e informações

Fonte: Elaborado pelo autor com base em Peoples (2013) e Dutton (2014).

A IoT, como apresentado no quadro 1, visa estender a capacidade de conectividade constante, de compartilhamento de dados e do controle a distância para o mundo físico (PEOPLES, 2013). Para alcançar tais pretensões a IoT capta as muitas permutações de detecção, marcação ou identificação de coisas através da internet, para finalidades como a identificação, monitoramento, detecção ou acionamento de outros dispositivos que estão *on-line*. Este conjunto de tecnologias permite que as pessoas ou outros objetos físicos armazenem, enviem e recebam informações de maneira que possam transformar a forma como as pessoas fazem as coisas e justificar a Internet das Coisas como um novo conceito tecnológico (DUTTON, 2014).

Devido ao emergente crescimento das tecnologias voltadas a IoT, múltiplas definições sobre a Internet das Coisas são encontradas na literatura atual, apresentando certa dificuldade em definir o que realmente esse conjunto de ferramentas significa, tornando-se necessário compreender suas ideias centrais, as implicações sociais, econômicas e técnicas que podem surgir por meio da sua implementação e uso (ZORZI, 2010; VASSEUR et al., 2011; DUTTON, 2014; SAXBY, 2015).

A razão para a existência dessas dificuldades está presente na interpretação sintática do termo Internet das Coisas, tratando-se de dois conceitos capazes de conduzir a interpretações diferenciadas sendo que o primeiro termo, internet, conduz a um olhar voltado para a rede que a Internet das Coisas é capaz de gerar, enquanto o segundo termo, coisas, conduz a um olhar voltado para algo genérico sendo capaz de ser integrado em um panorama mais comum (ATZORI; IERA; MORABITO, 2010).

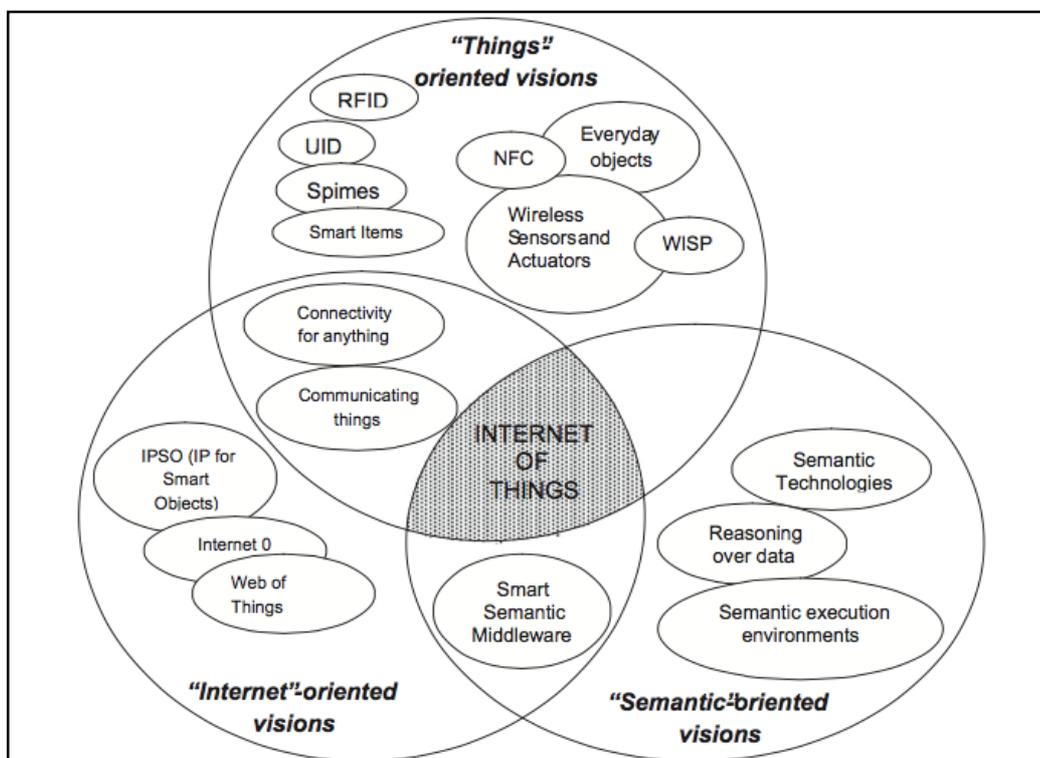
Estas diferenças nas visões a respeito da Internet das Coisas são oriundas das diversas iniciativas e interesses relacionados a este fenômeno, sejam alianças empresariais, órgãos de pesquisa ou agências reguladoras, cada um abordando esse fenômeno partindo de sua linha de atuação, interesse e finalidade, seja orientada a internet ou orientada as coisas (BRODY, 2015).

Tendo em tela o contexto construído até aqui, assume-se que ao unir os termos e apresenta-los como Internet das Coisas constrói-se um significado que conduz ao nível de ruptura de inovação na comunicação moderna. Assim a Internet das Coisas traduz-se em uma rede mundial de objetos interligados exclusivamente endereçáveis, com base em protocolos de comunicação padrão (LI; DA XU; ZHAO, 2014).

Tal realidade constrói-se em torno de um número indefinido de objetos envolvidos no processo, implicando na coleta, troca, armazenamento e interpretações de informações de múltiplas fontes originadas das atividades de pessoas e máquinas, levando diretamente para uma nova maneira de enxergar tais tecnologias, numa perspectiva orientada à Internet das Coisas (ASHRAF; HABAEBI, 2015).

Atzori, Iera e Morabito (2010) destacam tais visões da IoT defendendo que devesse considerar a Internet das Coisas por meio da convergência dessas três visões, como apresentado na figura 2.

**Figura 2:** Visões da Internet das Coisas



Fonte: Atzori, Iera e Morabito, 2010.

A primeira visão apresenta uma perspectiva orientada às coisas, trata-se de uma visão considerada pelos autores como mais simplista, visto que preocupa-se inicialmente com itens que podem ser considerados básicos como a tecnologia *Radio Frequency IDentification* - RFID, sensores *Wireless*<sup>3</sup> e equipamentos de tecnologia *Near Field Communication* - NFC<sup>4</sup>, tornando estes, componentes chave para a plena

<sup>3</sup> Estrutura de comunicação sem fio

<sup>4</sup> Comunicação por campo de proximidade

implantação da visão IoT, contudo a IoT contempla uma condição mais ampla e complexa do que a ideia de uma mera identificação de coisas.

Numa segunda visão, que está orientada a internet, destina os esforços da IoT para a criação de ambientes inteligentes, em que as coisas podem se comunicar automaticamente umas com as outras e com outras pessoas, aprimorando serviços e produtos já existentes e fornecendo novos a fim de gerar novos benefícios para a sociedade. Vasseur e Dunkels (2010) propõem um conceito de ambiente inteligente baseado na visão da Internet das Coisas como uma infraestrutura global que conecta objetos físicos e virtuais, capazes de incluir redes já existentes, novas evoluções pelas quais a internet ainda passará. Neste sentido, a IoT torna-se geradora de um ambiente virtual chamado de ambiente inteligente, com capacidade natural de implementação de serviços e aplicações caracterizados por um elevado grau de gerenciamento de dados e informações de forma autônoma e ininterrupta. Tais características surgem como o traço de união que interliga a primeira visão voltada as coisas com a segunda visão que centraliza a internet no panorama da IoT.

No constante a terceira visão, aquela orientada à semântica, preocupa-se com as questões relacionadas com a forma de coletar, armazenar, conectar, pesquisar e organizar as informações geradas pela Internet das Coisas, defendendo que os desafios constantes nessas ações devem constar nas discussões primárias em relação a IoT devido aos desafios que agregam e a sua complexidade. Neste contexto, a visão orientada à semântica desempenha um papel-chave tornando-se crucial para a construção de soluções capazes de explorar e modelar de forma apropriada os dados e informações gerados pela IoT, construindo e possibilitando a interpretação e a estrutura de comunicação da Internet das Coisas (ATZORI; IERA; MORABITO, 2010).

Diante de distintas visões de um todo que constitui a Internet das Coisas, Li, Da Xu e Zhao (2014) definem a Internet das Coisas como um conjunto de aplicações habilitados para a Internet com base em objetos físicos e o meio ambiente integrado aos da rede de informação. Definição esta, que será adotada nesta pesquisa por melhor contemplar o entendimento das três visões apresentadas.

A IoT consiste nos protocolos e tecnologias relacionadas que permitem que elementos diferentes se comuniquem através de canais de comunicações eletrônicas, com ou sem fio, numa rede de troca de dados e informações compostas por coisas e

peças (VALÉRY, 2012). Logo, como salienta Dutton (2014) a IoT destaca-se por permitir que informações eletrônicas passem a serem transmitidas por objetos físicos, como quando eles se movem através do espaço, de forma semelhante as redes sem fios que transmitem sinais eletrônicos, criando uma nova dimensão para a concepção e utilização da internet.

Diante da existência de distintas visões a respeito da Internet das Coisas, pode-se questionar se o advento da IoT pode ser encarado como um novo posicionamento tecnológico ou apenas como uma maneira reorganizada de utilizar os recursos já existentes na internet. Na próxima seção, uma discussão a respeito dos elementos que podem ser considerados para compreender a Internet das Coisas como um fenômeno essencialmente inovador será apresentada.

## 2. 1. 2 Internet das Coisas como novo posicionamento tecnológico

A próxima grande inovação da sociedade moderna será a plena implementação da Internet das Coisas, conectar não apenas as pessoas, mas também máquinas, coisas e objetos inteligentes, graças à conectividade sem fio (DUTTON, 2014). A comunicação entre coisas e pessoas será possível independentemente das circunstâncias de local e de forma, apresentando um novo posicionamento tecnológico na comunicação moderna (ROMAN; NAJERA; LOPEZ, 2011). Possibilitado por uma variedade de dispositivos conectados e identificados, torna-se possível perceber eventos e alterações dentro do chamado ambiente inteligente (CHABRIDON, *et al.*, 2014).

Apesar desses novos aspectos atribuídos a IoT, há um debate contínuo sobre se este é verdadeiramente um novo desenvolvimento tecnológico ou apenas uma iniciativa da indústria para promover e vender produtos e serviços remodelados como inovação, enquanto para outros trata-se de um desvio de sistemas tecnológicos já existentes no passado (KRÜCKEN, 2003).

Vários fatores que compõem o posicionamento tecnológico da Internet das Coisas, tais como a conectividade sem fio, os sensores, os dispositivos de captação e a tecnologia RFID, são tecnologias em estágios relativamente avançados e estáveis de utilização que estão sendo combinadas de novas maneiras (DUTTON, 2014).

No entanto, estas tecnologias que antes eram utilizadas com o foco no desenvolvimento de aplicações que buscavam conectar pessoas por meio de

mensagens eletrônicas e conferências, passam a focar seu desenvolvimento em colocar dispositivos *on-line* interligados com outros dispositivos. Desta forma, a IoT redireciona a atenção das aplicações tecnológicas para as relações constituídas entre pessoa-coisa, coisa-pessoa e entre coisa-coisa, configurado o ambiente de comunicação inteligente composto por pessoas e coisas (LI; DA XU; ZHAO, 2014).

O poder dessa visão evidencia-se pela ascensão dos novos modelos de negócios e soluções que são criados por meio da IoT, tais como as cidades inteligentes, os transporte inteligente, as casas inteligentes e em áreas da indústria de manufatura, da logística, da segurança patrimonial, da saúde e do controle ambiental. Por isso, especialistas defendem que a Internet das Coisas é a maior inovação em comunicação desde a Web (VALÉRY, 2012; LI; DA XU; ZHAO, 2014; DUTTON, 2014).

O impacto social e organizacional que a IoT potencialmente provoca na utilização das TIC's pode reconfigurar a maneira como as pessoas lidam com as informações, como convivem, como recebem e fornecem serviços e como utilizam as tecnologias existentes (PANG et al., 2015). Esperar que tais inovações pautadas na Internet das Coisas aconteçam justifica-se por uma série de características, sendo em primeiro lugar a flexibilidade que a IoT apresenta, sustentada pelas variadas combinações de tecnologias e soluções que podem ser aplicadas de variadas maneiras e adequadas a variados contextos, além dos constantes aperfeiçoamentos pelos quais componentes chaves da IoT passam para ampliar sua capacidade, vida útil e escala de produção, de maneira a possibilitar novas áreas de aplicação em potencial (DUTTON, 2014).

Segundo, é importante destacar que a IoT nem sempre faz algo inteiramente novo, mas faz as coisas mais próximas em tempo real e em um maior nível de precisão do que já foi feito antes. Em terceiro lugar, a IoT posiciona a partilha de dados no epicentro da sua aplicabilidade, tornando essencial a integração dos dados em diferentes setores e serviços já existentes e que venham a serem criados no futuro (DUTTON, 2014; ASHRAF; HABAEBI, 2015).

Entretanto, a ideia de compartilhar dados que foram coletados para um propósito específico, com o intuito de apoiar outro propósito distinto está repleto de novas questões de ordem ética, de ordem política e de ordem prática, mas a ideia de compartilhamento é fundamental para permitir que a IoT seja capaz de suportar aplicações que envolvem o conhecimento e o compartilhado de informações.

Combinar os dados de diferentes indivíduos torna-se a chave para o pleno funcionamento da IoT (DUTTON, 2014).

Não obstante ao entendimento dos autores (VALÉRY, 2012; LI; DA XU; ZHAO, 2014; DUTTON, 2014; PANG et al., 2015) essa pesquisa aceita a concepção de que a Internet das Coisas deve ser compreendida como um novo posicionamento tecnológico que abre possibilidades novas e significativamente melhoradas, podendo serem aplicadas em diversos contextos, sejam estes ambientes domésticos ou de negócios, como apresentados na sessão a seguir.

## 2. 2 O ambiente inteligente da Internet das Coisas

Ambientes inteligentes são ambientes nos quais a tecnologia da IoT é usada para melhorar as atividades comuns, sejam estas em ambientes domésticos e destinados ao lazer ou em ambientes profissionais (STEVENTON; WRIGHT, 2010). As seções seguintes estão destinadas a ilustrar cenários de aplicações da Internet das Coisas por meios de diferentes componentes da IoT e por diferentes níveis de melhoria das atividades tecnologicamente aprimoradas por soluções advindas dela.

### 2. 2. 1 A IoT no ambiente doméstico

A seguir, serão ilustrados cenários de aplicação da Internet das Coisas em uso doméstico, com a interação entre diferentes situações do cotidiano das pessoas e suas possibilidades individuais e sociais, por meios de diferentes componentes da IoT.

O conceito de casa inteligente refere-se à integração de tecnologia e serviços através de rede doméstica para uma melhor qualidade de vida. As casas inteligentes permitem a automação e controle do ambiente da casa a partir de dispositivos, como equipamentos de cozinha automáticos, iluminação e portas automáticas, controladores de temperatura interna, controladores de temperatura de água, dispositivos de segurança e vigilância interna (DARIANIAN; MICHAEL, 2008).

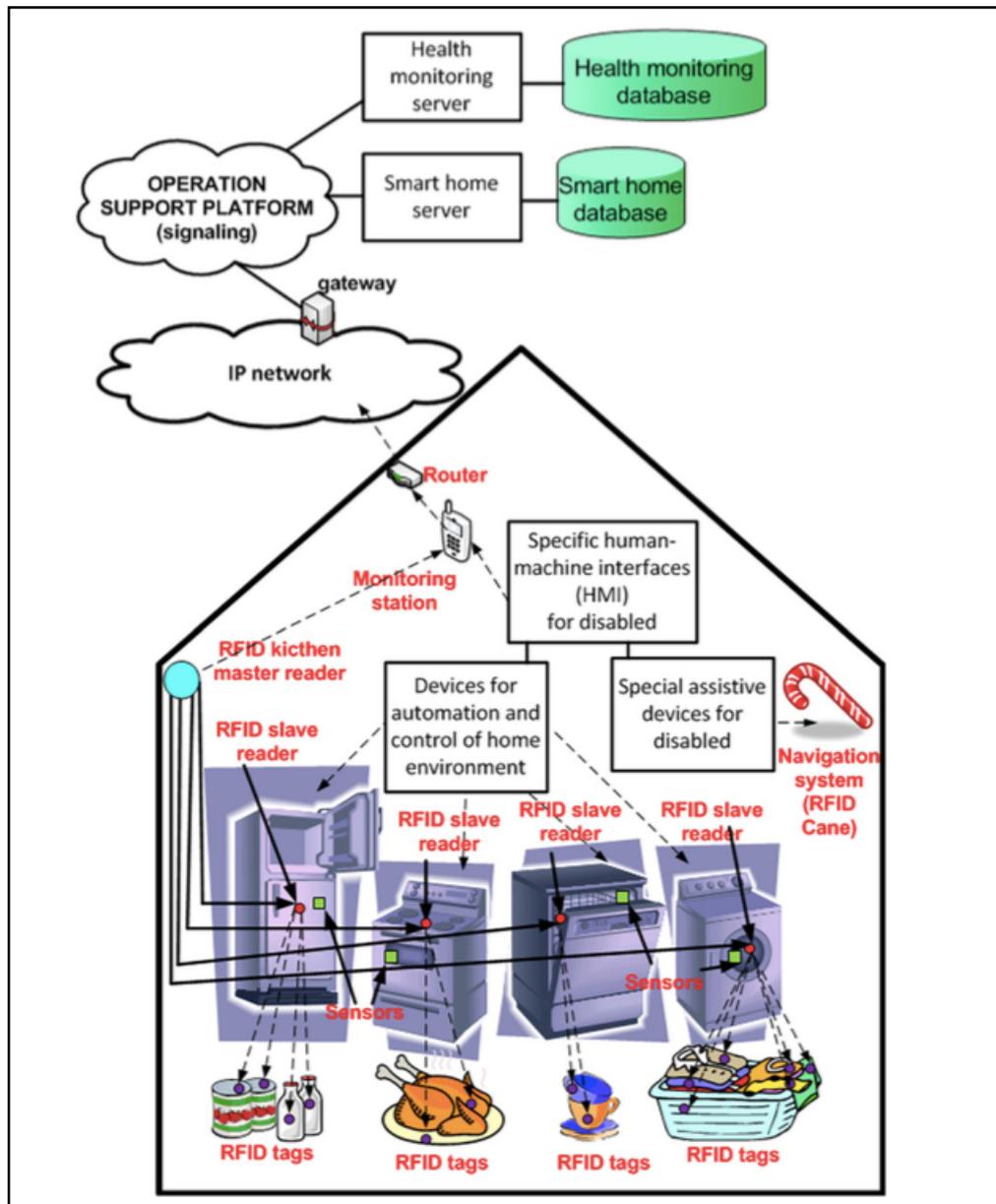
Estes dispositivos voltados para a automação residencial são formados por sensores e atuadores embutidos em produtos, eletrodomésticos ou móveis. Os sensores monitoram as condições ambientais, processam, recolhem informações e cooperam com outras unidades através de uma rede sem fio. Os dados coletados são

processados por um servidor para fornecer serviços adequados para o usuário. Se forem detectados eventos que dão origem a situações de alarme, atuadores são acionados para lidar com a atual situação de emergência, como incidentes de assalto ou incêndio (DOMINGO, 2012).

A integração de RFID no ambiente doméstico inteligente é também essencial para fins de identificação e rastreamento. Darianian e Michael (2008) propõem uma arquitetura RFID em que leitores secundários integrados nos eletrodomésticos comunicam-se com os leitores móveis e com um leitor mestre que é conectado ao servidor da casa inteligente. Tais interligações podem ser aplicadas as tarefas diárias da casa, como por exemplo, lavagem de roupas.

A figura 3 ilustra uma situação em que as etiquetas RFID ligadas a roupa contêm dados sobre a cor, material e programa de lavagem adequado. Se a quantidade de roupas sujas detectadas por um leitor de RFID atinge um determinado patamar predefinido, um alerta é automaticamente enviado e um programa de lavagem inteligente é sugerido para economizar energia. O leitor também verifica a compatibilidade entre a roupa quando a máquina de lavar estiver sendo carregada. As roupas sujas deixadas para a próxima lavagem também são monitoradas com o auxílio do servidor da casa inteligente e de um banco de dados.

Figura 3: A IoT nas tarefas diárias



Fonte: Domingo, (2012).

Outras aplicações domésticas inteligentes que combinam serviços de internet com identificação RFID podem ser desenvolvidas, tais como os sensores de uma geladeira inteligente em conjunto com os das prateleiras de determinada dispensa que podem comunicarem-se com o leitor mestre na cozinha para sugerir receitas culinárias com base na preferência do residente e em suas condições de saúde, como alergias alimentares, colesterol, diabetes, etc, invocando os serviços *web* que fornecem busca e *download* da receita. Os servidores de vigilância da saúde e de banco de dados são úteis para monitorar e registrar as condições de saúde dos

residentes. Os servidores de casas inteligentes e banco de dados também são úteis para registrar a lista do residente de alimentos necessários e assim como a atual disponibilidade desses itens para compará-los e gerar uma lista de compras automaticamente (DOMINGO, 2012).

Buckl et al. (2009) apresentam possibilidades de implementação de uma lógica de automação com o propósito de otimizar o consumo de energia ao longo do dia, de acordo com os horários de picos de consumo, obtidos a partir de um serviço *web* externo. O consumo de energia na casa é diminuído desligando aparelhos fora de uso remotamente e desativando o fornecimento de energia em casos específicos em que a casa se encontra desabitada, como períodos de férias.

As novas possibilidades criadas com a implementação de ambientes inteligentes permitem que as interações entre as pessoas aconteçam automaticamente por intermédio da transmissão autônoma de informações. Esta transmissão torna possível informar o que os usuários estão fazendo ou o que os usuários fizeram, por meio da coleta e transmissão de dados de suas movimentações diárias, suas viagens, lugares frequentados e atividades físicas. A disponibilização dessas informações permitirá que usuários próximos de hábitos semelhantes possam interagir, transformando aplicações de uso doméstico em aplicações sociais (WELBOURNE, 2009).

Atori, Iera e Morabito (2010) destacam certas aplicações que estão mais presentes na Internet das Coisas no uso doméstico, focadas nas utilidades sociais, como a consulta a históricos sobre objetos e dados de eventos que permitem que os usuários estudem as tendências em suas atividades ao longo do tempo. Plataformas com esse tipo de característica podem ser úteis para a criação de atividades de longo prazo, tais como projetos colaborativos. A capacidade de memória digital pode ser construída gravando e exibindo eventos, gerando um registro para posterior leitura e análise. Desta forma, os usuários podem verificar o histórico e constatar como, com quem, com o quê e onde o tempo está sendo gasto.

Outra utilidade doméstica e social da IoT apresentada por Atori, Iera e Morabito (2010), e corroborada por Li, Da Xu e Zhao (2014) é o motor de busca para as coisas, uma ferramenta que ajuda a encontrar objetos cuja localização não é conhecida ou foi esquecida pelo usuário.

Este tipo de aplicação, em seu formato mais simples, baseia-se em uma aplicação capaz de permitir aos usuários a visualização da última localização registrada pela coisa que está sendo procurada, ou em caso de coisas imóveis, sua geolocalização particular. Uma versão mais personalizada desse tipo de ferramenta atribui personalização ao usuário, dando-lhe condição de criar requisitos específicos para a coisa que está sendo buscada, definindo atributos de notificação em relação ao horário, clima, localização e velocidade de deslocamento, permitindo que o usuário receba notificações sempre que o item pesquisado atender aos requisitos pré-estabelecidos (WELBOURNE, 2009; CHAOUCHI, 2013)

Por meio de uma aplicação voltada para a segurança antifurto, é possível monitorar a retirada de objetos de determinados locais como casas e escritórios, a retirada sem prévia autorização de saída, gera uma notificação de saída não autorizada o que indica uma possível ação de furto do objeto monitorado, podendo a aplicação ser configurada para notificar automaticamente agentes de segurança particulares ou a polícia local (ATORI; IERA; MORABITO, 2010; CHAOUCHI, 2013).

Tais possibilidades de aplicação das tecnologias pautadas na IoT, como as aqui apresentadas, tende a expandir-se com a consolidação dessas tecnologias pela indústria e áreas de negócios impulsionadores do consumo em massa (WEBER; WEBER, 2010). Para tanto, as soluções baseadas na tecnologia da Internet das Coisas precisam consolidarem-se nos negócios, onde, assim como no ambiente doméstico, possuem uma série de cenários e oportunidades possíveis, como apresentado na seção a seguir.

## 2. 2. 2 Negócios inteligentes

O conceito de Internet das Coisas, com sua visão de objetos conectados à internet com variadas capacidades, poderia impulsionar o papel das TIC's como inovação em uma variedade de mercados de aplicação existentes e que ainda serão criados. Para que isto aconteça um dos pilares tecnológicos da Internet das Coisas, ou seja, a tecnologia RFID, já foi incorporado em uma ampla gama de produtos. De acordo com Miorandi (2012), o número de etiquetas RFID comercializadas no ano de 2011 chegaram a 2,88 bilhões e geraram um valor estimado de 5,84 bilhões de dólares.

O aumento no uso de RFID, que possibilita a utilização da Internet das Coisas, não é simplesmente um resultado de impulso tecnológico, já que também é incentivado pela força do mercado, uma vez que as empresas estão cada vez mais percebendo os benefícios comerciais de aplicações que podem ser realizados com a tecnologia da Internet das Coisas (BRODY; PURESWARAN, 2015).

A evolução da IoT tende a seguir o caminho de evolução dos telefones celulares. No final do ano de 2009 havia 5,9 bilhões de telefones celulares ativos, número crescente impulsionado pela necessidade de se comunicar em qualquer lugar e a qualquer hora. Acreditando em uma evolução da conectividade em igual volume sendo trazida para objetos do cotidiano, tais como geladeiras, carros, chaves, etc., uma vez que irá ser ativado por intermédio da IoT, este cenário configura-se como uma grande oportunidade de mercado para a Internet das Coisas, relacionados com a possibilidade de colocar em rede as coisas inteligentes e de fornecer aplicações capazes de alavancar essa expansão da conectividade (ATZORI; IERA; MORABITO, 2010).

Em termos de campos de aplicação e setores do mercado em que as soluções da Internet das Coisas podem proporcionar vantagens competitivas sobre os concorrentes, Miorandi et al. (2012) identificam seis mercados que podem desempenhar um papel de liderança na adoção de tecnologias da Internet das Coisas sendo eles, o de casas inteligentes e gestão de condomínios, as cidades inteligentes, o monitoramento ambiental, o de cuidados de saúde, os negócios inteligentes voltados à gestão de produtos e o de segurança e vigilância. A seguir, discute-se brevemente a relevância e o potencial impacto das tecnologias da Internet das Coisas sobre a competitividade das empresas nesses mercados.

As casas e condomínios inteligentes são caracterizadas pelas aplicações avançadas da IoT, que podem viabilizar a redução do consumo e do desperdício de recursos como água e eletricidade, como também promover a melhoria do bem-estar coletivo sejam para trabalhadores em um escritório ou para moradores em casas e apartamentos particulares. Nesta aplicação, um papel chave é desempenhado pelos sensores que são usados para monitorar o consumo de recursos e para detectar de maneira proativa as necessidades das pessoas em tempo real (MIORANDI et al., 2012; BRODY; PURESWARAN, 2015).

Tal cenário integra uma série de diferentes subsistemas, e, portanto, requer um alto nível de padronização para garantir a operabilidade interna e fornecer ao

sistema central a capacidade de raciocinar de um modo cooperativo e distribuído, garantindo assim a melhor decisão a respeito de recursos sob controle do sistema como a iluminação, o aquecimento, a refrigeração, etc, alinhando os recursos em relação as necessidades e expectativas dos usuários, que por sua vez são estritamente entrelaçadas com as atividades que realizam ou pretendem realizar (WELBOURNE, 2009; MIORANDI et al., 2012).

O termo cidades inteligentes é utilizado para designar o ecossistema emergente por meio da implantação de infraestrutura de comunicação avançada e novos serviços sobre cenários de toda a cidade. Por meio de serviços avançados, é realmente possível otimizar o uso da infraestrutura física da cidade como as redes de estradas, as redes de energia, as redes de abastecimento de água, etc, melhorando a qualidade de vida para os seus cidadãos (SAXBY, 2015).

As tecnologias da IoT podem encontrar aplicações neste cenário de cidade inteligente, onde a IoT pode ser usada para fornecer sistemas avançados de controle de tráfego, por exemplo. Através da Internet das Coisas é possível monitorar o tráfego de automóveis nas grandes cidades ou rodovias e implantar serviços que ofereçam sugestões de rotas de tráfego para evitar congestionamentos. Nesta perspectiva, os carros são monitorados como objetos inteligentes em movimento das rodovias e estradas (ZORZI, 2010).

Além disso, Li, Da Xu e Zhao (2014) destacam que sistemas de estacionamento inteligentes podem possibilitar o monitoramento de vagas disponíveis e fornecer sugestões aos motoristas em tempo real de onde é o local mais indicado para estacionar, melhorando assim a mobilidade na área urbana. Em complemento, os sensores podem monitorar o fluxo de tráfego de veículos nas rodovias e recuperar informações agregadas, como velocidade e número médio de carros.

Sensores podem detectar o nível de poluição do ar, reunindo informações sobre poluição atmosférica, tal como o nível de dióxido de carbono e entregar essas informações a agências de saúde. Estes sensores podem, também, serem usados em um ambiente forense, através da detecção de violações da lei submetendo os dados relevantes para as agências de aplicação da lei e órgãos responsáveis, a fim de identificar o infrator, ou para armazenar informações que serão fornecidas em caso de acidente, para posterior análise (STEVENTON; WRIGHT, 2010; DOMINGO, 2012).

O monitoramento ambiental apresenta-se como uma área a ser explorada pela IoT por meio de sua capacidade de detecção, de distribuição da informação e de

autogestão que esta tecnologia pode proporcionar, acompanhando variações de temperatura, vento, precipitação, altura das águas em rios, entre outros. O processamento de informação em tempo real, juntamente com a capacidade de um grande número de dispositivos comunicarem-se entre eles, fornece uma plataforma sólida para detectar e monitorar anomalias que podem indicar perigo para a vida humana e animal. A grande implantação de dispositivos miniaturizados pode permitir o acesso a áreas críticas, em que a presença de operadores humanos podem não representar uma opção viável como em regiões vulcânicas, abismos oceânicos ou áreas remotas e de deserto (FLOERKEMEIER; RODUNER; LAMPE, 2007; DOMINGO, 2012).

Nesta perspectiva, as tecnologias da Internet das Coisas possibilitam o desenvolvimento de uma nova geração de sistemas de monitoramento e apoio à decisão, fornecendo capacidade avançada de acompanhamento em tempo real (ATZORI; IERA ; MORABITO, 2010).

Outro caso em que a capacidade de detecção de dispositivos da IoT apoia a segurança ambiental é representada por detecção de incêndio. Quando um conjunto de sensores detecta a possível presença de fogo através do monitoramento da temperatura um alarme é enviado diretamente para o corpo de bombeiros em um curto espaço de tempo, juntamente com outros parâmetros que são úteis para a tomada de decisão e de apoio, tais como a descrição da área, a possível presença de pessoas, de materiais inflamáveis, etc. Claramente, a resposta rápida tem a consequência de salvar vidas, mitigando o dano à propriedade ou a vegetação e, em geral, reduzindo o nível de desastre. Muitos outros cenários relacionados com a proteção civil podem lucrar com as tecnologias da Internet das Coisas, pela sua capacidade de acessar dados ambientais em tempo real sobre áreas de grande escala permitindo a absorção de estratégias eficazes de coordenação entre as equipes de salvamento (FLOERKEMEIER; RODUNER; LAMPE, 2007).

O setor de saúde configura-se como um campo em que as tecnologias da Internet das Coisas podem encontrar uma série de aplicações. Tais aplicações podem ser utilizadas para melhorar as soluções já existentes e criar novas possibilidades, fornecendo uma visão abrangente dos parâmetros de saúde, desencadeando uma intervenção pela equipe médica após a detecção de condições que podem levar à deterioração da saúde, realizando assim o cuidado preventivo (DOMINGO, 2012).

Domingo (2012) destaca ainda outro setor de aplicação relevante que se refere aos cuidados pessoais com a saúde e o bem-estar. O uso de sensores portáteis, juntamente com aplicações adequadas executados em dispositivos de computação pessoal possibilitarão que as pessoas passem a rastrear suas atividades diárias, verificando quanto a pessoa já caminhou, quantas calorias já foram queimadas, quanto tempo de exercícios físicos já foram realizados, etc, fornecendo sugestões para melhorar o seu estilo de vida e prevenir o aparecimento de problemas de saúde.

No tocante a gestão de negócios, em especial a gestão de estoque, Atori, Iera e Morabito (2010) e Miorandi et al. (2012) afirmam que a tecnologia RFID já é utilizada em diversos setores no auxílio a gestão de inventário, em toda a cadeia de fornecimento e entrega. Isso depende da capacidade deste tipo de tecnologia para identificar e fornecer suporte para rastreamento de mercadorias, porém, as aplicações RFID são construídas de forma não integrada, integrando sistemas fechados de gestão. RFID são habitualmente utilizados para monitorar e gerenciar a circulação de produtos através de uma cadeia de abastecimento, tendo etiquetas ligadas diretamente aos itens enquanto os leitores são fixados na instalação de monitoramento. As tecnologias da Internet das Coisas podem fornecer maior flexibilidade em termos de posições dos leitores, enquanto, ao mesmo tempo podem permitir interoperabilidade entre aplicações baseadas em RFID utilizadas por diferentes membros da cadeia de suprimento que lidam com o produto ao longo das várias fases do seu ciclo de vida.

Na indústria varejista, Li, Da Xu e Zhao (2014) afirmam que a IoT pode ser aplicada para monitorar a disponibilidade do produto em tempo real e manter controle preciso sobre o estoque. Tornando possível o fornecimento de pós-venda ágil e personalizado por possibilitar ao cliente obter todos os dados dos produtos comprados automaticamente. Além disso, tecnologias de identificação podem ajudar a limitar roubos reduzindo custos com sinistro e seguro, além do combate a falsificação, fornecendo produtos com um identificador único. Por seu turno, sensores em combinação com a tecnologia RFID podem permitir que o processo de produção do produto ganhe maior controle de qualidade, possibilitando o acompanhamento do produto até o consumidor final, sendo possível acompanhar até mesmo sua vida útil de prateleira no caso de alimentos e produtos facilmente perecíveis.

Nos setores de segurança e vigilância eletrônica, as tecnologias da IoT podem ser a chave para melhorar substancialmente o desempenho das soluções atuais, capazes de reduzir o custo para as empresas e aumentar o benefício para os usuários assim como a sua privacidade (BRODY; PURESWARAN, 2015).

Dentre as possibilidades, sensores que monitoram a presença de substâncias químicas e produtos inflamáveis, assim como os que monitoram comportamentos suspeitos e hostis, podem ser utilizados para monitorar de forma autônoma ambientes públicos e industriais, com o objetivo de evitar dano ao patrimônio e acidentes. Tais sensores, ao detectar situações fora da normalidade programada, emitem alertas para autoridades e para órgãos responsáveis otimizando o tempo de resposta a possíveis incidentes (BRODY; PURESWARAN, 2015).

Quando usado em conjunto com sistemas de controle de acesso baseado em função, as tecnologias da Internet das Coisas podem proporcionar alto nível de flexibilidade, sendo capaz de lidar com as políticas de acesso para diferentes áreas de um complexo industrial, de um edifício do governo ou de áreas de uso público que podem mudar ao longo do tempo devido a mudança de fatores como rotas de acesso, papel do usuário, informações contextuais. Também neste mercado as vantagens são em termos de funcionalidade aprimorada, melhor aceitação do usuário, através da redução do uso de câmeras, redução de custos operacionais e aumento da flexibilidade em um ambiente de constante mudança (FLOERKEMEIER, RODUNER; LAMPE, 2007).

Espera-se neste panorama de possibilidades apresentado que a adoção IoT seja fortemente impulsionada pelas necessidades dinâmicas do mercado, ao mesmo tempo em que as indústrias de TIC, organismos de normalização e os formuladores de políticas públicas estejam a realizar uma série de iniciativas para orientar o processo de desenvolvimento da Internet das Coisas com o objetivo de maximizar o seu valor socioeconômico (MIORANDI et al., 2012).

## 2.3 Privacidade e a IoT

Diante do volume de dados e informações que a implementação da Internet das Coisas pode disponibilizar, seja por meio das pessoas ou de maneira autônoma por intermédio dos objetos inteligentes, a privacidade demanda atenção de envolvidos, sejam pessoas, órgãos reguladores, empresas e governos. Tal

preocupação com a privacidade, assim como os elementos que a formam são discutidos na seção a seguir de maneira a melhor fundamentar a preocupação central deste projeto de pesquisa.

### 2. 3. 1 Privacidade na era da informação

A privacidade é uma das principais preocupações éticas dos usuários com relação à Internet das Coisas e é uma questão crucial que pode limitar a implementação da visão IoT (MIORANDI et al., 2012). O controle deste novo ambiente complexo, a troca de dados invisível e constante entre as coisas e as pessoas, e entre as coisas e outras coisas, precisa ocorrer de maneira anônima, sem o conhecimento dos proprietários e criadores desses dados. A própria escala e capacidade das novas tecnologias vai ampliar este problema, pois controlar os dados recolhidos por todos os objetos conectados que compõem o ambiente inteligente torna-se uma tarefa chave para o desenvolvimento dessa nova realidade (CHABRIDON et al., 2014).

Krause (2009) apresenta uma análise aprofundada das questões de privacidade no domínio da computação ambígua e ao revisar antigas referências a privacidade em textos de lei percebe que ainda hoje não se está claro exatamente qual é o significado da privacidade, especialmente com os novos usos oferecidos pelas Tecnologias da Informação e da Comunicação atuais. Krause e Hochstatter (2005) apontam a privacidade como o direito de ser deixado em paz. Por seu turno, Krause (2009) afirma que preservar a privacidade através do isolamento não é mais uma opção no mundo da informação e da comunicação existente no século XXI.

Segundo Chabridon et al. (2014) a privacidade é agora geralmente percebida pelos usuários como uma expectativa de permanecer num estado de proteção sem ter que o perseguir ativamente. Os usuários só demonstram preocupação efetiva com a privacidade quando sentem que esta foi violada. Marx (2001) identifica quatro linhas de fronteira pessoais que são percebidas como violações de privacidade, sendo estas apresentadas a seguir no quadro 2.

**Quadro 2: Linhas de fronteiras pessoais**

<b>Linha de fronteira</b>	<b>Descrição</b>
<b>A fronteira natural</b>	Impede a presença de sentimentos e/ou emoções não sendo percebidos através dos sentidos humanos. Paredes, portas, roupas, escuridão, cartas seladas, telefone e e-mail representam fronteiras naturais para observação.
<b>A fronteira social</b>	Envolve expectativas que as pessoas com certos papéis sociais como médicos, membros do clero, advogados e outros não irão divulgar informações confidenciais a eles fornecidas pelas pessoas envolvidas.
<b>A fronteira espacial ou temporal</b>	Separa a informação dos vários períodos ou aspectos da vida da pessoa.
<b>A fronteira dos efeitos transitórios</b>	Supõem que a interação e a comunicação são efêmeros e transitórios como ações que se esperam, sendo facilmente esquecidas em um curto espaço de tempo.

Fonte: Elaborado pelo autor com base em Marx (2001).

Solove (2006) argumenta que nenhuma definição de privacidade é capaz de atender a todos os aspectos compreendidos pela privacidade, mas sim que existem várias formas de privacidade, propondo uma taxonomia de privacidade com uma visão geral das atividades que possam levar a sua violação, sendo elas:

- A coleta de informações, que embora a informação geralmente seja recolhida com o consentimento do proprietário da informação, cobranças forçadas ou interrogatórios podem levar a violação da privacidade da pessoa.
- A disseminação da informação, quando realizada pode incorrer no estropolamento da confidencialidade, podendo tal situação ser gerada de múltiplas formas.
- A divulgação, que pode acontecer com a publicação de fatos verídicos, no entanto, tais fatos podem afetar a reputação da pessoa, por meio da exposição de dados e informações privados que possam vir a serem vinculados.
- E a invasão, que pode ocorrer nos dados pessoais por meio do acesso intrusivo em sua personalidade e através da interferência decisória.

Como foi assinalado por Krause (2009), embora esta taxonomia pretenda ser utilizada para proteção legal, poderá também ser útil para as tecnologias. Os

fornecedores de tecnologia devem analisar sistematicamente se algum *software* ou tecnologia pode aumentar as chances de tal problema ocorrer, e buscar desenvolver soluções que possam mitigar tais chances (CHABRIDON et al., 2014).

Chabridon et al. (2014) baseados nos estudos de Danezis e Gurses (2010) categorizam aspectos de privacidade em três classes distintas, sendo elas a privacidade como confidencialidade, a privacidade como controle e a privacidade como transparência, cada categoria com distinções entre si, como apresentado a seguir.

A privacidade como confidencialidade é normalmente presente de alguma forma em tecnologias existente, como o primeiro objetivo é proteger a privacidade dos dados pessoais evitando que estes sejam acessados por pessoas não autorizadas. Se os dados pessoais se tornam públicos, a confidencialidade e privacidade, portanto, são perdidas. Privacidade como confidencialidade representa as soluções para garantir o anonimato dos dados, das comunicações (SAXBY, 2015).

A abordagem anonimato parte da ideia de que o indivíduo não pode ser identificado dentro de um conjunto de usuários. No entanto, o grau de anonimato considerado suficiente em um caso específico de uso particular depende diretamente de consequências legais e sociais causadas por uma possível violação de dados e ainda é uma questão em aberto como destacam Chabridon et al. (2014). Diferencial de privacidade tem como objetivo fornecer meios para maximizar a precisão das consultas a partir de bases de dados estatísticos, minimizando as chances de identificar os seus registros (VAIDYA, 2012).

A geração desse anonimato nas comunicações visa proteger os dados de tráfego e esconder quem fala com quem na rede. Mesmo que o conteúdo de uma comunicação seja mantido em sigilo, informações confidenciais podem ser vazadas por dados de tráfego que incluem locais e as identidades das partes em comunicação, tempo, frequência e volume da comunicação. Por isto, fornecer comunicação anônima é um desafio uma vez que muitos protocolos de comunicação usam identificadores únicos (MATOS; 2012; VAIDYA, 2012).

A abordagem da privacidade como controle refere-se à capacidade de controlar o que acontece com os dados pessoais para evitar abusos por parte de terceiros. Isto requerer tecnologias para a especificação e aplicação de políticas de privacidade. Para direcionar estes aspectos de controle, Wang e Kobsa (2008) identificam 11 princípios fundamentais da privacidade, com apresentado no quadro 3.

**Quadro 3:** Princípios fundamentais da privacidade

<b>Princípio</b>	<b>Descrição</b>
<b>A consciência de utilização</b>	Baseada em declarações claras e bem detalhadas das políticas de privacidade.
<b>A minimização dos dados</b>	Busca avaliar a necessidade, eficácia e proporcionalidade de novas tecnologias antes de sua implantação, dando preferência a soluções menos invasivas.
<b>A especificação de objetivos</b>	Observa a finalidade para qual os dados estão sendo coletados.
<b>A limitação de coleta</b>	Objetiva definir os limites para a coleta de dados a ser realizada.
<b>A limitação de uso</b>	Definisse a fim de evitar que dados sejam usados ou divulgados para fins que não tenham sido especificados no momento da coleta.
<b>A proteção de transferência</b>	Deve ser definida para evitar que dados sejam transferidos caso a garantia de proteção adequada não possa ser mantida.
<b>A capacidade de escolha e consentimento</b>	Baseia-se no princípio de que os indivíduos devem possuir a capacidade de decidir sobre a coleta, uso e divulgação de seus dados.
<b>O acesso</b>	Garante que as pessoas podem verificar seus dados armazenados.
<b>A integridade</b>	Princípio base para garantir que os dados recolhidos serão destinados para a finalidade a que se destinam.
<b>A segurança</b>	Garantia de que os dados estão fora de risco de perda, acesso não autorizado, uso indevido, modificação ou divulgação não autorizada.
<b>A aplicação</b>	Preocupa-se diretamente com a existência de mecanismos que façam cumprir os princípios da privacidade.

Fonte: Elaborado pelo autor com base em Wang e Kobsa (2008).

Na sequência, a abordagem da privacidade como transparência pretende aprimorar a compreensão das pessoas e seu controle sobre os dados que são coletados, tal pretensão traduz-se na aplicação de quatro características definidas por Castellucia et al. (2011) como cruciais para que essa tecnologia alcance a transparência, sendo elas:

- A capacidade de fornecer informações sobre a coleta, destinação, armazenamento e processamento dos dados;
- A capacidade de fornecer relatórios capazes de informar quais dados foram divulgados, para quais finalidades e sobre o abrigo de quais políticas;
- A capacidade de proporcionar acesso *on-line* pelos seus proprietários aos dados;

- E a capacidade de ajudar o usuário a prever possíveis oportunidades e riscos relevantes a sua privacidade.

Privacidade como transparência é uma questão importante porque a maioria das tecnologias são inúteis se as pessoas não podem usá-los de forma eficiente. Privacidade como a transparência é ainda mais crítico para os sistemas distribuídos baseados na IoT do que as aplicações onipresentes baseadas na *web* existentes. Os usuários, não só terão que controlar os dados pessoais que podem ser propagados a partir dos terminais com os quais eles interagem diretamente, como *smartphone* e *tablets*, mas também terão que lidar com o controle dos dados produzidos automaticamente pelas coisas conectadas que eles possuem, que os cercam ou que estão localizados em ambientes que frequentam como *shopping*, escritório, consultório e outros (VAIDYA, 2012; SAXBY, 2015).

Vislumbrando a complexidade das questões que envolvem a privacidade, algumas abordagens tentam envolver os utilizadores na gestão da privacidade propondo a melhoria da compreensão dos usuários a respeito das implicações de privacidade, fornecendo-lhes *feedback*, relatórios de privacidade para permitirem que os usuários definam seus controles primários e, em seguida, verifiquem a forma como os seus dados privados são vistos a partir do ponto de vista das outras pessoas (CHABRIDON et al., 2014).

No entanto Weber e Weber (2010) salientam que a preocupação com a privacidade das informações faz com que o risco de um controle rigoroso por parte do proprietário, possa colocar em risco a veracidade de certas atividades, ocultando informações que possam vir a indicar determinadas atividades criminosas. Neste sentido a privacidade das informações pode, a longo prazo, não ser necessariamente indissolúvel, portanto, o quadro jurídico a ser elaborado para lidar com esse fenômeno precisará está adaptado a está nova realidade. Na próxima seção será apresentado um panorama geral das principais iniciativas legislativas em relação a privacidade.

### 2. 3. 2 Perspectiva legal da privacidade de informação

Conceber as inovações transformadoras que a Internet das Coisas potencialmente pode gerar sem refletir sobre os riscos sociais, éticos e legais que as envolvem torna-se inexecutável quando se trata de aplicações que possibilitam o

controle, a localização e o monitoramento da saúde das pessoas, entre outras variadas possibilidades. A maioria das preocupações centralizam-se nos riscos de comprometer a privacidade pessoal de um indivíduo, criando sistemas que tornam a proteção de dados cada vez mais crítico ao abrigo do direito e das leis existentes (DUTTON, 2014).

Privacidade e vigilância estão entre uma série de riscos sociais e éticos ligados à Internet das Coisas (SPIEKERMANN, 2013). As populações de grandes metrópoles já são monitoradas diariamente por câmeras de vigilância e o advento da IoT tem a capacidade de alargar ainda mais este potencial de vigilância pública e privada, levando-a a locais ainda não alcançados pela indústria de segurança tradicional (WEBER; WEBER, 2010).

Tal expectativa demonstra que as questões de privacidade são difíceis de resolver e tendem a tornar-se mais complexas, com o acréscimo de novas questões, como a confiança levantada por Guerra et al. (2002), em que salientavam naquela época haver uma tensão na relação de confiança destacando que a recolha e disponibilização de dados pode criar problemas de confiança em termos de privacidade, sendo esta, facilmente identificada como uma preocupação que impede os consumidores de usar a internet para transações. Desta forma, há uma tensão na confiança entre a privacidade e identidade, a ausência de dados completos, como uma prestação de contas limitada, prejudica a confiança, mas a coleta de dados detalhados cria problemas de confiança em relação ao uso dos mesmos.

Estas questões estão intimamente ligadas as incertezas sobre a propriedade e controle dos dados e informações que as aplicações da IoT podem gerar. Atribuir propriedade dos dados recolhidos por meio da IoT em vários contextos que envolvem múltiplos atores, apresenta-se como um dos desafios iniciais para esse tipo de aplicação (ROCHELANDET; TAI, 2012).

Dutton (2014) comenta que em contextos tradicionais os direitos de autor dos dados e das informações geradas por máquinas são atribuídos ao operador do equipamento, contudo, tal entendimento pode não ser plenamente aplicado a redes de sensores de funcionamento autônomo. Da mesma forma, em alguns outros contextos, a propriedade é contestada, tal como com os dados de saúde, que podem pertencer simultaneamente a pacientes, hospitais, laboratórios e a controladores, em

situações de pesquisa em que novos diagnósticos são criados, novos medicamentos testados e dados genômicos são registrados (DUTTON, 2005).

A Internet das Coisas tende a ampliar essa construção colaborativa, compartilhando aplicações e dados não apenas entre prestadores de serviços e consumidores, mas entre setores e cadeias produtivas inteiras, tornando ainda mais complexa a definição de propriedade (ASHRAF; HABAEBI, 2015).

A possibilidade de roubo ou outro acesso não autorizado aos dados ou sistemas desenvolvidos em torno da IoT significa que a segurança cibernética precisa ser vista como prioridade para a implementação de sistemas confiáveis. Estes sistemas têm de ser seguros a fim de estarem preparados para os mais variados cenários como em caso de catástrofes naturais, de intrusão por quaisquer usuários não autorizados, para situações de violação de dados acidentais por parte de funcionários bem-intencionados com autorização a manipular dados (KIRK, 2012).

Evidencia-se que a implementação da arquitetura IoT ressalta uma série de desafios legais. Por tratar-se de um fenômeno global, existe a necessidade de estabelecer diretrizes gerais que possam ser adotadas pela legislação de todos os países a fim de proporcionar a padronização das ações. Weber e Weber (2010) destacam algumas das principais legislações que norteiam questões centrais a respeito da IoT.

O direito à privacidade, a proteção da privacidade individual livre de vigilância nacional e internacional, o rápido progresso alcançado no domínio das tecnologias da informação e, em particular, sobre a evolução, como as impressões digitais, o monitoramento de rede, os sistemas de bio-consciência, o processamento eletrônico de dados e a criação de extensas bases de dados, têm facilitado não só a coleta e armazenamento, mas também o processamento e interligação dos dados pessoais (ROCHELANDET; TAI, 2012; SAXBY, 2015).

Estes desenvolvimentos oferecem vantagens consideráveis em termos de eficiência e produtividade, mas também implica riscos potenciais. A tecnologia moderna oferece, em poucos segundos, o acesso a quantidades ilimitadas de dados pessoais e estabelece a possibilidade de criar perfis dos usuários, através da combinação de diferentes arquivos de dados, este é facilitado pela tecnologia de vigilância, podendo causar um aumento considerável no desrespeito a privacidade individual (GREER, 2006).

Neste sentido, diversos organismos internacionais preocupam-se com tais riscos definido em suas legislações o direito a privacidade, como o apresentado pelo art. 12 da Declaração Universal dos Direitos Humanos - DUDH, Art. 17 do Pacto Internacional sobre os Direitos Civis e Políticos - PIDCP, bem como o art. 8º da Convenção Europeia dos Direitos do Homem - CEDH (ALVES, 1999; PIOVESAN, 2006; COMPARATO, 2010). Além disso, no que concerne à Internet das Coisas como evolução da internet atual, a iniciativa brasileira recente, do marco civil da internet, busca garantir a segurança do usuário, sua privacidade e a neutralidade da rede (URNAUER; MENNA BARRETO, 2015).

Na sociedade da informação a proteção de dados pessoais deve ser considerado uma questão-chave, tendo em conta que o direito a privacidade e a proteção dos dados deve ser uma garantia essencial para o equilíbrio entre a vida privada, no que diz respeito as liberdades individuais e as exigências de segurança, em relação à necessidade de existir informações disponíveis (WEBER, 2010).

Dentro dessa realidade Steffek e Nanz (2008) apresentam uma concepção de liberdade para a IoT, defendendo que os usuários devem ter total controle sobre etiquetas e sensores, podendo desativá-los sempre que desejarem, a fim de controlar a maneira como seus dados são coletados e utilizados. No que diz respeito a aplicação dos direitos humanos, parte-se do entendimento da proteção dos direitos individuais da pessoa humana, de sua individualidade perante a sociedade, resguardando-a das arbitrariedades do Estado e dos órgãos governamentais. Para tanto parte-se do princípio que é da sociedade civil organizada que terá que surgir as iniciativas de regulamentação da privacidade na IoT (COMPARATO, 2010).

Por encontrar-se em estado inicial de desenvolvimento de aplicações, a IoT ainda não possui uma realidade de auto-regulamentação única, sendo regulada por variados padrões de negócios promovidos pela indústria que os conduzem a práticas de auto-regulamentação da informação. Esta existência de auto-regulação na IoT coincide com as experiências feitas no campo da governança da internet em geral (WEBER; WEBER, 2010; BRODY; PURESWARAN, 2015).

Um acordo internacional vinculativo que abrange privacidade e proteção de dados ainda não existe. Mesmo que os instrumentos internacionais de direitos humanos tendam a vislumbrar na essência do uso da internet uma solução válida para a IoT, pelo menos até certo ponto, tais mecanismos não podem ser considerados

suficientes, contudo, desde que não seja percebido como uma garantia universal, esta pode ser uma iniciativa pertinente para o fenômeno da Internet das Coisas (ATZORI; IERA ; MORABITO, 2010).

Portanto, é amplamente aceito que a co-regulação é necessária para garantir a implementação de princípios eficazes de privacidade no ambiente inteligente. Possíveis elementos de um sistema de auto-regulação podem incluir códigos de conduta que contenham regras de boas práticas elaboradas em conformidade com a proteção da privacidade das pessoas, o estabelecimento de procedimentos de controle interno, o ajuste de linhas diretas para lidar com as reclamações do público, e proteção de dados transparente (WEBER, 2010).

Tais iniciativas de padronização global da proteção da privacidade na IoT são de suma importância para a consolidação desse tipo de tecnologia, contudo, é importante destacar que a preocupação com a segurança e a privacidade apresentadas pelas pessoas, não são idênticas em localidades distintas do globo, o que torna a aplicação dos princípios gerais difíceis, principalmente quando trata-se de atividades comerciais entre diferentes países (WEBER, 2010; ROCHELANDET; TAI, 2012). Diante dessa realidade, Weber e Weber (2010) salientam que um quadro jurídico de base deve ser introduzido por um legislador internacional, no entanto, os detalhes das regras jurídicas devem ser desenvolvidos pelo setor privado.

*“Design é função, não forma”.*

(Steve Jobs)

### 3. PROCEDIMENTOS METODOLÓGICOS

Este estudo tem como objetivo investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Cosias ao fornecerem informações pessoais em ambientes inteligentes. Para auxiliar no alcance de tal objetivo, esta seção apresentará as escolhas metodológicas eleitas para a operacionalização da pesquisa, explicitando quanto ao posicionamento epistemológico, a natureza e os meios da pesquisa, bem com a escolha do instrumento de coleta de dados, as técnicas de tratamento e análise dos dados e, por fim, os cuidados metodológicos.

#### 3. 1 Posicionamento Epistemológico da Pesquisa

Epistemologia é originalmente uma palavra grega que pode ser entendida como a ciência que estuda a ciência, ou seja, a ciência que é capaz de analisar como o conhecimento é construído (CHAUÍ, 2002). O posicionamento epistemológico claro e bem definido por parte do pesquisador permite a estruturação da pesquisa que se pretende empreender, tornando-se possível definir o objetivo científico adequado e a problemática a ser investigada (IVONE, 2005). Para essa pesquisa, posicionar-se epistemologicamente tem caráter essencial para definir a ótica pela qual o fenômeno será analisado, orientando desta forma todo o processo de investigação e como os resultados encontrados serão analisados.

Dentre as diversas abordagens epistemológicas de pesquisa que podem ser adotadas pela ciência da administração, essa pesquisa buscou se enquadrar na mais apropriada para a natureza do estudo e para o perfil do pesquisador, como recomenda Burrell e Morgan (1979) e Chauí (2002). Neste sentido, observa-se entre as abordagens mais presentes em pesquisa em administração, as óticas estruturalista, sistêmica, crítica e positivista, como afirma Rocha, Araújo e Marques (2012).

A ótica da epistemologia estruturalista de pesquisa defende que o conhecimento se desenvolve pela explicação analítica de um dado fenômeno, objeto de pesquisa, durante sua decomposição e análise profunda (BURRELL; MORGAN, 1979). Uma pesquisa essencialmente estruturalista possui entre seus elementos

centrais o esforço em decompor o objeto analisado buscando encontrar o ponto central da questão por meio das partes separadas do objeto estudado. Admite-se que o fenômeno estudado é sempre variável e, portanto, não explicativo, sendo necessário a exploração profunda de seus elementos, por isto defende-se a persistência da busca pelo não superficial a fim de construir uma ordem lógica pela análise das partes mínimas do objeto (ROCHA; ARAÚJO; MARQUES, 2012).

Posicionando-se de encontro a essa visão, a visão sistêmica considera privilegiada a análise do todo sobre as partes. O pensamento sistêmico defende que o fenômeno só pode ser explicado se o todo for considerado, tendo como defesa a lógica na qual o objeto de pesquisa só existe se o todo existir (SCHRADER; MALWITZ-SCHÜTTE; SELL, 1974). Neste sentido, o posicionamento sistêmico defende a crença de que não é possível alcançar a compreensão completa do objeto pesquisado pela soma das partes, sendo necessário uma análise integrada do todo ao qual está ligado (SERVA, 2014).

O positivismo enquanto visão epistemológica, segundo Trivinos (1987), está pautado na busca de explicações dos fenômenos estudados por meio da análise das relações que os fenômenos possuem, pela observação e pelo processamento dos fatos para compreensão do que está sendo estudado. Trata-se de um posicionamento objetivo, em que a teoria é utilizada para elaborar hipóteses que serão testadas para afirmar ou negar a teoria em análise (BURRELL; MORGAN, 1979).

Rocha, Araújo e Marques (2012) apresentam três regras principais, definidas por Demo (1981), pelas quais o positivismo pode ser caracterizado. O fenomenalismo, que é a primeira regra, define a não aceitação pela pesquisa positivista da distinção entre fenômeno e a essência, tornando-se possível, dessa forma, o desvendar de um fenômeno por meio da observação superficial do acontecimento. Logo, o importante na investigação é aquilo que pode ser observado.

A segunda regra, o nominalismo, estabelece que a conceituação é tomada apenas como nomes a objetos concretos, evitando a nominalização de coisas não observáveis, neste sentido o nominalismo valida na pesquisa positivista apenas fenômenos concretos e observáveis evitando a absorção de informações abstratas incompatíveis com a nominalização.

E, por fim, a regra da neutralidade científica que defende que o papel do cientista é exprimir a realidade e não a julgar como certa ou errada. Partindo desta lógica, a regra da neutralidade defende a ideia de que não há influência dos valores

do pesquisador sobre o fenômeno pesquisado, sendo este fator suprimido e retirado da observação, não sendo sequer levado em consideração na análise.

Contrariando as abordagens já apresentadas, a visão crítica questiona o fundamento estático da realidade, partindo do pressuposto que o fenômeno estudado está sempre em formação e nunca deve ser enxergado como algo fechado e acabado. Esta visão defende a ideia de continuidade de ações que são herdadas de contextos anteriores, pelas quais se constituem os conflitos como elementos desestruturantes, entendidos como condicionantes para a mudança junto com fatores externos (BURRELL; MORGAN, 1979).

Essa pesquisa buscou investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Coisas ao fornecerem informações pessoais em ambientes inteligentes, analisando as relações identificadas no processo de fornecimento de informações por meio dos dados levantados em campo. Neste contexto, a investigação posicionou-se mais adequadamente na visão epistemológica positivista, uma vez que se buscou encontrar resposta para a problemática da pesquisa por meio da análise objetiva dos dados coletados em campo.

### 3. 2 Caracterização da Pesquisa

A ciência da Administração caracteriza-se pela sua natureza social e aplicada, essencialmente focada na compreensão e resolução de problemas de ordem prática e operacional. Mas não obstante a finalidade prática da pesquisa, ela pode contribuir para o aperfeiçoamento de teorias e para a compreensão de elementos ainda pouco explicados pelas teorias existentes (ZANELLA, 2009).

Para que tal contribuição aconteça, é necessário que a pesquisa parta de um arcabouço teórico já existente sobre os elementos a serem analisados e que uma pesquisa de campo seja implementada a fim de gerar novos achados capazes de contribuir com a teoria existente. Pesquisas que adotam estas características em sua implementação são definidas como pesquisas teórico-empíricas (LEWIS; THORNHILL; SAUNDERS, 2007). Por essa pesquisa caracterizar-se de maneira semelhante, posicionou-se de igual forma como um estudo teórico-empírico.

Sendo a Internet das Coisas ainda pouco explorada do ponto de vista das ciências em Administração, existem poucas informações disponíveis que auxiliem na

compreensão dos aspectos que determinam a ação dos usuários ao fornecerem suas informações em ambientes inteligentes, por isto, observou-se a necessidade de realizar uma pesquisa empírica capaz de auxiliar na compreensão das particularidades dos usuários da IoT partindo de uma perspectiva diferente da apresentada pelas ciências da computação.

Tendo em vista essa necessidade, o estudo caracterizou-se como uma pesquisa de natureza exploratória-descritiva, por buscar descobrir novas possibilidades, identificar quais situações, eventos, atitudes ou opiniões estão manifestos em uma população, tentando descrever como o fenômeno se comporta em determinado contexto.

### 3. 3 Método de Pesquisa

A escolha do método por parte do pesquisador está intimamente ligada aos seus domínios de técnicas de análise dos dados que serão coletados no campo. Esta escolha pode revelar aspectos de sua visão de mundo, sua preocupação com o referencial teórico, a relação do investigador com realidade e toda a lógica da pesquisa a ser implementada (FREITAS et al., 2000). Para tanto, Zanella (2009) destaca que em relação aos métodos as pesquisas são classificadas de três maneiras: qualitativas, quantitativas e quali-quantitativa ou método misto.

A pesquisa qualitativa, originalmente advinda da Sociologia e da Antropologia, fundamenta-se em análises de natureza não quantificadas, não utilizando instrumental estatístico para analisar os dados coletados. A pesquisa qualitativa possui uma natureza essencialmente descritiva por se propor a descrever fenômenos por meio dos significados encontrados, que são comumente expressos em formas de transcrições de entrevistas, narrativas, declarações, fotografias, desenhos, documentos, diários pessoais, dentre outros. Assim, mantém-se sempre, por parte do pesquisador, a preocupação em compreender e interpretar o fenômeno a partir do ponto de vista dos participantes (ZANELLA, 2009).

Por seu turno, a pesquisa quantitativa caracteriza-se pela utilização de instrumentos estatísticos, seja na coleta como no tratamento dos dados, sendo capaz de medir relações entre variáveis (ZANELLA, 2009). Tal tipo de método é apropriado quando o foco de interesse da pesquisa encontra-se em explicar o que está acontecendo, como acontece ou porque acontece dado fenômeno.

A pesquisa quantitativa pode configurar-se essencialmente de natureza explanatória quando busca testar relações causais; exploratória, quando busca familiarizar-se com algum fenômeno em específico; e descritiva quando está focada em identificar situações, eventos, atitudes ou opiniões manifestadas em um determinado grupo ou população (FREITAS et al., 2000)

Já a pesquisa qualitativa-quantitativa, ou pesquisa mista, caracteriza-se pela junção de características dos dois métodos mencionados a pouco, podendo ser realizada em sua etapa inicial de maneira quantitativa e torna-se qualitativa em uma segunda etapa, ou ao contrário a depender do fenômeno que esteja sendo estudado, podendo ainda constituírem análises conjuntas no decorrer da pesquisa (LEWIS; THORNHILL; SAUNDERS, 2007).

Partindo destas concepções, a presente pesquisa configurou-se como uma pesquisa quantitativa por buscar com sua aplicação mensurar aspectos que determinem o fornecimento de informações por parte dos usuários de tecnologias inteligentes fazendo uso da mensuração dos dados coletados em campo.

### 3. 4 Estratégia da Pesquisa

A pesquisa de campo estabelece-se por meio da observação dos fatos tal como ocorrem, não permitindo isolar e controlar variáveis do fenômeno, mas perceber e estudar as relações estabelecidas (LEWIS; THORNHILL; SAUNDERS, 2007). Tendo em vista a natureza dos objetivos deste estudo, que buscou a identificação, descrição e análise do fenômeno estudado, foi adotada como estratégia a pesquisa de campo do tipo *survey*, estratégia que combina técnicas de coleta e análise estatísticas para para melhor estudar o fenômeno como ele ocorrer naturalmente partindo da percepção dos respondentes, sendo capaz de avaliar de maneira ampla as relações causais entre os aspectos que determinam as ações analisadas e os dados e informações que os respondentes disponibilizam.

#### 3. 4. 1 Universo e Público Alvo

O universo de abrangência dessa pesquisa foi formado pelas pessoas que utilizam objetos de tecnologia inteligentes de qualquer natureza como relógio

Inteligente (*Smart Watch*), aparelhos de TV Inteligente (*Smart TV*), telefone Inteligente (*SmartPhone*), aparelho de som Inteligente (*Smart Stereo*), Pulseira Inteligente (*Smart Bracelet*), GPS Inteligente (*GPS Smart*), agenda Inteligente (*Smart Calendar*), óculos Inteligente (*Smart Glasses*), itens de vestuário esportivo como camisetas, viseiras, bonés, tênis, bermudas, entre outros dispositivos com capacidade de interação através da IoT, seja em ambiente doméstico ou profissional, que residam em território brasileiro.

O processo de definição da amostra, como salienta Freitas et al. (2000), é composto pela definição da população-alvo, seguida da definição do contexto de amostragem, da unidade de amostragem, pela seleção de amostragem, pelo tamanho da amostra ou pela execução do processo de amostragem. Seguindo essa composição, nesta investigação, a pesquisa de campo teve como público alvo os usuários de objetos inteligentes conectados a internet cadastrados nos bancos de dados da [survio.com](http://survio.com) e da [surveymonkey.com](http://surveymonkey.com) em território brasileiro.

#### 3. 4. 2 Amostra

De acordo com Freitas et al (2000), a amostra de pesquisa pode ser definida de duas formas, a amostra probabilista que proporciona representatividade da população estudada e a amostra não probabilística que é definida a partir de um cenário específico assumindo determinadas limitações, as características que diferenciam os dois tipos de amostra são expostas a seguir.

A amostra probabilística representa-se pelo fato de todos os elementos da amostra possuírem a mesma chance de serem escolhidos, resultando em uma amostra representativa da população, resultado da seleção randômica dos respondentes (FREITAS et al., 2000). Esse tipo de amostra pode ser classificada como estratificada e não estratificada, sendo que sua diferença principal está na preocupação que se deve ter, por parte do pesquisador, em manter presente todos os fatores intervenientes da população.

A amostra probabilística pode ser caracterizada de duas maneiras: a primeira como amostra proporcional, que é caracterizada por fornecer igual representatividade para cada estrato da amostra no universo; e a segunda, como amostra não proporcional, onde não há obrigatoriedade de fornecer igualdade de

representatividade para os estratos que compõem o universo da pesquisa (LEWIS; THORNHILL; SAUNDERS, 2007).

Por sua vez, a amostra não probabilística é obtida na definição de algum tipo de cenário, por meio da escolha de critérios específicos, assumindo que nem todos os elementos da população têm a mesma chance de serem selecionados, tornando dessa forma a generalização dos resultados limitada. Este tipo de amostra torna-se recomendável quando os respondentes da pesquisa são de difícil acesso ou identificação (FREITAS et al., 2000).

A amostra não probabilística pode ser dividida em seis tipos gerais: a amostra por conveniência, em que os participantes são escolhidos por estarem disponíveis; a amostra entre os mais similares ou mais diferentes, definida pela similaridade ou singularidade dos participantes; a amostra por cotas, tipo de amostra proporcionalmente escolhida para atender determinado critério; a amostra bola de neve, meio pelo qual os primeiros entrevistados vão indicando outros a participarem da pesquisa; a amostra de casos críticos, critério pelo qual os participantes da pesquisa são definidos por representarem o foco da pesquisa; e a amostra por casos típicos, em que a amostra é definida pelos casos típicos, excluindo casos extremos a amostra (BUSSAB; MORETTIN, 2003).

A população brasileira já possui aproximadamente 306 milhões de dispositivos conectáveis a internet, isto é, 3 dispositivos para cada 2 habitantes (MEIRELLES, 2014), tendo sido a população brasileira alvo desta pesquisa, enquadrando-se a amostra com não probabilística, por não dar condição a toda a população nacional, usuária de algum tipo de tecnologia que suporte a capacidade de interação proporcionada pela IoT, de participar da pesquisa.

Definiu-se a amostra como por conveniência, por ser adotados respondentes que estão disponíveis em dois bancos de dados já estabelecidos, tal escolha se deu pela inviabilidade de identificar em todas as regiões do país pessoas que possuam as características necessárias para participar da pesquisa, pela dispersão geográfica dos respondentes para atender a abrangência nacional da pesquisa e pela natureza do corte-transversal da pesquisa, restringindo o tempo de coleta dos dados para 45 dias, tornando inviável a pesquisa por meio presencial.

A amostra também se caracterizou como amostra entre mais similares, por tratar-se de um grupo específico de pessoas que utilizam um determinado tipo de

tecnologia específica em dado contexto específico, restringindo a pesquisa aos usuários de algum tipo de tecnologia IoT em alguma estância.

### 3. 5 Coleta dos Dados

O instrumento de coleta de dados mais utilizado em pesquisa do tipo *survey*, como destaca Bruni (2012), é o questionário. Segundo Zanella (2009), tal instrumento pode conter perguntas descritivas com o propósito de descrever a realidade que está sendo pesquisada; perguntas comportamentais, a fim de conhecer o comportamento do fenômeno que está sendo estudado; e perguntas preferências que avaliam condições ou circunstâncias em relação a problemática da pesquisa. Para esta pesquisa, o questionário será adotado como ferramenta de coleta de dados que contém perguntas de natureza descritiva, comportamental e perguntas preferenciais, podendo serem respondidas de forma objetiva.

Freitas et al. (2000) ressaltam que a escolha do instrumento de coleta de dados deve estar ligada diretamente à capacidade do mesmo de levantar os insumos necessários para o alcance dos objetivos da pesquisa. Havendo a necessidade de explorar os aspectos determinantes da ação das pessoas que fornecem informações por meio de objetos inteligentes, descrevendo como este fenômeno acontece e buscando analisar os possíveis aspectos determinantes, acreditou-se que o questionário é o instrumento de coleta de dados mais adequado para a implementação desta pesquisa.

Como destacam Bussab e Morettin (2003), deve-se adotar precauções na hora de conceber o questionário para não criar questões que excluam possíveis respostas e, por consequência, acabe por anular a possibilidade de realizar novas descobertas na pesquisa. Assim como é necessário seguir uma estrutura lógica que possibilite ao respondente lidar de forma autônoma com o questionário por meio de orientações a respeito de seu preenchimento, da sua sequência lógica e da clareza das perguntas.

Os enunciados das perguntas constantes no instrumento de coleta de dados devem ser construídos com base na revisão da literatura pertinente ao fenômeno estudado e devem estar alinhados com os objetivos definidos no escopo da pesquisa, esses cuidados validam a utilização do instrumento de coleta de dados

adotado e permite ao pesquisador verificar a consistência do instrumento em relação aos objetivos da pesquisa (TRIVISIOS, 1987).

Seguindo o exposto pelos autores, apresenta-se no quadro 4, o quadro de consistência das questões existentes no questionário, que pode ser verificado no apêndice A, a fim de relacionar os enunciados com os objetivos da pesquisa e verificar seu alinhamento com a questão norteadora da proposta deste estudo.

**Quadro 4:** Quadro de Consistência do Instrumento de Coleta de Dados

<b>PROBLEMA</b>	<b>OBJETIVO GERAL</b>	<b>OBJETIVOS ESPECÍFICOS</b>	<b>INSTRUMENTO</b>	<b>QUESITO</b>
Quais aspectos determinam a ação das pessoas ao fornecerem informações pessoais em ambientes inteligentes?	Investigar os aspectos que determinam a ação das pessoas ao fornecerem informações pessoais em ambientes inteligentes.	- Identificar os tipos de tecnologias inteligentes utilizadas pelas pessoas;	Questionário	Itens de 5 a 7
		- Descrever as formas de uso cotidianas das tecnologias inteligentes;		Itens de 8 a 12
		- Identificar os tipos de dados e informações fornecidos em ambientes inteligentes;		Itens de 13 a 16
		- Analisar os aspectos determinantes para o fornecimento de dados e informações no ambiente inteligente		Itens 17 e 18

Fonte: Elaborado pelo autor (2016).

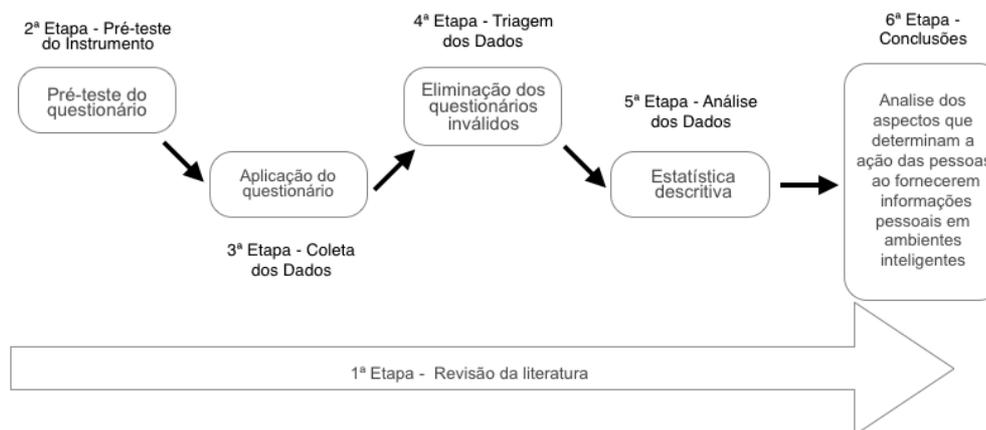
O quadro de consistência do instrumento de coleta de dados foi utilizado de igual maneira para auxiliar nos procedimentos práticos da pesquisa, por este motivo, é apresentado antes do desenho da pesquisa, visto que a consistência do instrumento escolhido norteia como serão implementadas as atividades da pesquisa, como será apresentado na seção a seguir.

### 3. 5. 1 Desenho da Pesquisa

O desenho da pesquisa tem o objetivo de ilustrar o fluxo de atividades que compõem sua implementação, apresentando visualmente as operações que a

compõem, neste caso em específico, o desenho apresentado na figura 4, representa o desenho da pesquisa em sua sequência lógica.

**Figura 4:** Desenho da pesquisa



Fonte: Elaborado pelo autor (2016).

A primeira etapa da pesquisa compreendeu a fase de levantamento inicial da literatura existente sobre a temática investigada, este levantamento inicial, foi que forneceu as bases necessárias para a construção do modelo de instrumento de coleta dos dados em campo. Contudo a revisão da literatura pertinente, não se limitou ao momento inicial da pesquisa, tornando-se contínua durante todo o processo de investigação, até o confronto dos resultados para a construção das conclusões da pesquisa.

A segunda etapa da pesquisa, atribuiu-se ao pré-teste do instrumento, que foi realizado em três fases: a primeira fase, por meio da avaliação de três especialistas, doutores na linha de investigação que se seguiu essa pesquisa; a segunda fase, um teste de aplicação com 5 professores pesquisadores de áreas afins, com o objetivo de verificar a dualidade de conceitos com interpretações e aplicações distintas em outras áreas; a terceira fase, contemplou um teste de aplicação com 10 pessoas do público alvo da pesquisa para avaliar a dificuldade de interpretação dos enunciados e a auto aplicação do instrumento.

A coleta de dados, terceira etapa da pesquisa, tratou da aplicação do questionário. Sua aplicação foi realizada por meio das ferramentas de pesquisa *online* da [survio.com](http://survio.com) e da [surveymonkey.com](http://surveymonkey.com), plataformas nas quais o questionário

estiveram hospedado e pelas quais foram distribuídos para os respondentes em território nacional durante 45 dias, com o auxílio das ferramentas de divulgação de pesquisa a voluntários de ambas as plataformas.

Na quarta etapa da pesquisa, triagem dos dados, sobre a qual será tratado mais a fundo na sessão 3.6, após serem eliminados os questionários considerados inválidos, o conteúdo dos questionários seguiu para a análise quantitativa.

A quinta etapa da pesquisa, análise dos dados, se deu por meio da aplicação da estatística descritiva, pela qual se organizou os dados para identificar as características da amostra e descrevê-la. Foram escolhidas dentre as variáveis definidas, as que se apresentaram representativas, tendo um volume de respondentes suficiente para a posterior análise.

Na conclusão, que se apresenta como última etapa da pesquisa, foram confrontados resultados oriundos da análise dos dados, em comparação aos resultados de estudos já existentes e da teoria que fala a respeito do tema estudado, a fim de alcançar a resposta para o problema dessa pesquisa, cumprindo assim seu objetivo central.

### 3.6 Tratamento dos Dados

O tratamento inicial dos dados coletados se deu por meio de uma triagem realizada no sistema de filtragem das plataformas da [survio.com](https://www.surveymonkey.com) e da [surveymonkey.com](https://www.surveymonkey.com), para eliminar questionários inválidos. Foram considerados questionários inválidos aqueles que por motivos específicos foram incapazes de inspirar confiança nas respostas como questionários incompletos, questionários cuja pergunta de verificação tenha sido respondida de forma incorreta e questionários que os respondentes tenham sinalizado não possuírem objetos inteligentes.

Após a filtragem inicial dos dados, realizados por meio das ferramentas das plataformas da [survio.com](https://www.surveymonkey.com) e da [surveymonkey.com](https://www.surveymonkey.com), utilizados para selecionar os questionários válidos, os dados brutos foram exportados para o software de produtividade Numbers da plataforma Appel iWork, para a descrição e caracterização da amostra, gerando gráficos que apresentaram o perfil dos respondentes, em relação ao gênero, a faixa etária, a região do país e ao nível de escolaridade.

Buscando atender aos objetivos específicos da proposta de pesquisa, foram gerados infográficos para apresentar os tipos de tecnologias inteligentes

utilizadas pelas pessoas participantes da pesquisa; as formas de uso cotidianas dessas tecnologias em ambientes profissionais e domésticos; os tipos de dados e de informações fornecidas pelas pessoas nos ambientes inteligentes; e os aspectos que determinam o fornecimento destes dados e informações. Estes infográficos além de fornecerem um panorama geral da amostra, também serão estratificados de acordo com a categorização da amostra, tendo seus resultados comparados em relação ao gênero, a faixa etária, a região do país e ao nível de escolaridade, mediante estatística simples.

### 3. 8 Cuidados Metodológicos

Buscando assegurar a realização da pesquisa, alguns cuidados metodológicos foram adotados para minimizar possíveis imprevistos em sua implementação. Desta forma, torna-se importante expor tais cuidados adotados na realização da pesquisa.

Especifica-se o cuidado em avaliar, no pré-teste, o formato de aplicação mais efetiva do questionário, para otimizar o nível de retorno e garantir volume de dados relevantes para análise.

Segundo, para evitar a perda irrecuperável de dados, todos os dados coletados para a pesquisa eram checados após o término da coleta e salvos na nuvem para garantir acesso facilitado em caso de problemas do dado em meio físico.

Por estar ciente da vital importância de garantir a relevância das respostas, os respondentes que indicarem não possuir, ou não utilizar nenhum tipo de objeto inteligente, foram retirados dos dados, assim como os questionários que não foram completamente respondidos.

E por último, para garantir que as informações coletadas fossem as mais completas possíveis, foi realizada uma análise do campo outros, disponibilizado nos itens do questionário a fim de identificar as informações relevantes que pudessem ser acrescentadas a análise, evitando possíveis vies do pesquisador que remetam a descobertas já esperadas.

*“Pensar é o trabalho mais difícil que existe.  
Talvez por isso tão poucos se dediquem a  
ele”.*

(Henry Ford)

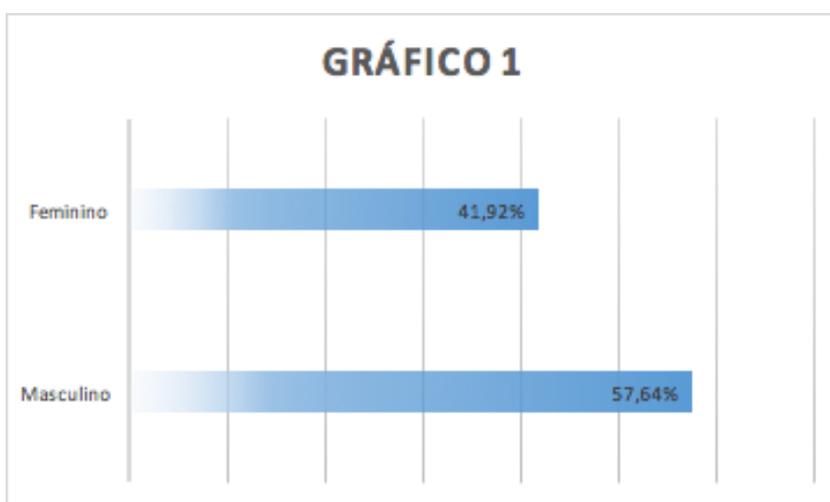
## 4 ANÁLISE DOS DADOS

Este capítulo apresentará a análise dos dados coletados em campo, sendo estruturado em cinco seções com vistas a expor os achados de modo didático e analisá-los a luz dos objetivos específicos definidos para o estudo. Desta forma, buscou-se comparar os resultados encontrados com a literatura que deu sustentação teórica para a investigação e identificar as especificidades da amostra em evidência. Com o intuito de explorar e descrever o conhecimento existente a respeito da relação de privacidade do usuário em ambientes inteligentes, assim como os aspectos elementares do uso de dispositivos inteligentes, essenciais para o desenvolvimento e implementação da Internet das Coisas.

### 4.1 Perfil dos respondentes

Buscando caracterizar a amostra que faz parte desta investigação, as questões de 1 a 4 do questionário dedicaram-se a traçar o perfil dos respondentes. Neste sentido o rol de sujeitos pesquisados caracteriza-se como uma amostra composta por 228 respondentes, conforme ilustrado no gráfico 1, numa distribuição de 41,92% de entrevistados do gênero feminino e 57,64% de entrevistados do gênero masculino.

**Gráfico 1:** Gênero dos respondentes



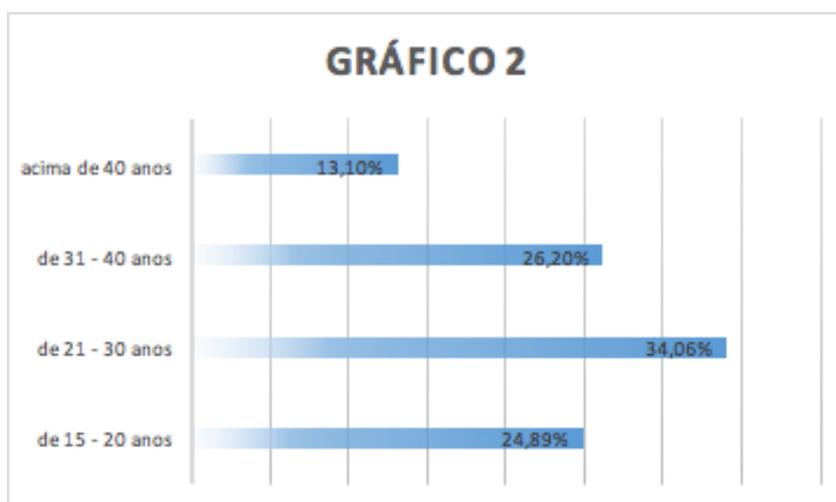
Fonte: Dados da Pesquisa (2016).

Estes dados iniciais se coadunam com o que apresenta Chabrindon (2014), ao afirmar que os avanços frequentes das tecnologias pessoais permitem o equilíbrio de gênero de seus usuários, não havendo grandes discrepâncias de gênero por parte do uso da tecnologia.

Embora ainda seja observada a predominância do gênero masculino entre os profissionais da área de tecnologia dentro e fora do país (WEBER, 2010; MEIRELLES, 2014), o atual equilíbrio no acesso e uso das tecnologias tem potencial para despertar maior interesse nas mulheres em adentrar nesse mercado. Ao mesmo tempo que, os atuais profissionais e empresas, devem pensar soluções em igual equilíbrio de gênero, visto que as mulheres já se apresentam como consumidoras igualmente ativas de dispositivos inteligentes.

Em relação a faixa etária dos respondentes, observou-se parcial equilíbrio entre a amostra, como apresentado no gráfico 2 logo adiante. Visualizando o resultado esperado, a maior incidência dos usuários se deu nas faixas etárias mais jovens com idade até os 30 anos que compreendeu 58,95% dos respondentes. No entanto, destaca-se a parcela de 13,10% dos respondentes na faixa etária acima dos 40, demonstrando que esta amostra se aproxima da tendência apresentada por Dutton (2005) ao destacar a popularização do uso da tecnologia entre as faixas etárias mais experientes.

**Gráfico 2:** Faixa etária

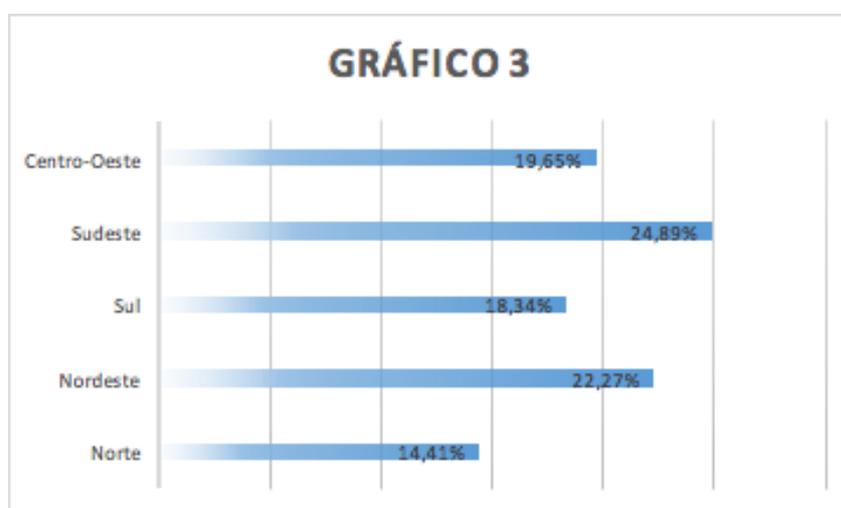


Fonte: Dados da Pesquisa (2016).

Este cenário promissor onde usuários em faixas etárias mais elevadas tem maior acesso a tecnologias inteligentes, têm potencial para tornar possível setores de aplicação da IoT voltados para cuidados com a saúde, acompanhamento médico e manutenção do bem-estar como já destacou Domingo (2012), ao sinalizar estas finalidades como potenciais nichos para a evolução contínua da IoT.

Com o intuito de buscar representatividade nacional, a pesquisa buscou coletar dados de usuários das cinco regiões do país, tendo sua distribuição percentual, apresentada no gráfico 3 na sequência.

**Gráfico 3:** Distribuição regional da amostra



Fonte: Dados da Pesquisa (2016).

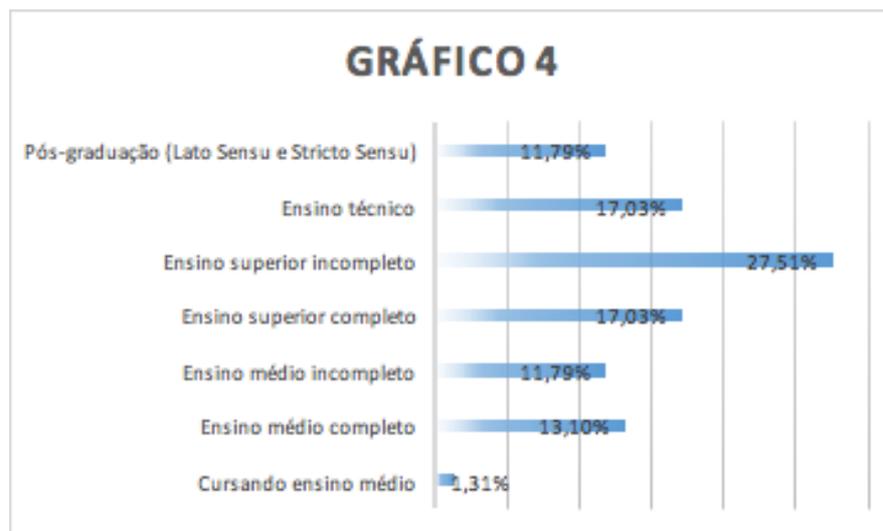
Dentre as regiões do país, destaca-se negativamente a região Norte com 14,41% dos respondentes, região do país onde mais houve dificuldade em coletar os dados e a maior incidência de questionários inválidos, sendo que a média de tempo de resposta do questionário nesta região foi a maior do país, chegando a dobrar em comparação com a região Nordeste que obteve o menor tempo de resposta por questionário válido.

Essa situação atribui-se ao fato da região apresentar os mais baixos índices de disseminação de tecnologia e de qualidade de sinal de conexão de internet do país (MEIRELLES, 2014). Isso deve ser observado de maneira preocupante do ponto de vista da disseminação das tecnologias IoT, por dependerem diretamente da conexão a internet para a ampliação das soluções existentes e para a manutenção da

existência de dispositivos inteligentes ativos (ROMAN; NAJERA; LOPEZ, 2011).

No que tange ao grau de escolaridade dos respondentes, observou-se que o uso desse tipo de tecnologia no país é democrático, como verificou-se no gráfico 4, visto que não foi identificado um grau de escolaridade que possa ser destacado como predominante na pesquisa.

**Gráfico 4:** Grau de escolaridade dos respondentes



Fonte: Dados da Pesquisa (2016).

No entanto, cabe destacar que entre os respondentes que possuem grau médio de escolaridade, ou seja, ensino médio completo e ensino superior incompleto, juntos representam 40,61% da amostra analisada, demonstrando que um percentual considerável dos usuários desse tipo de artefato, possui um grau de instrução acima do ensino básico. O grau de instrução mediano dos usuários favorece a construção de um ambiente homogêneo e unificado como destaca Vasseur e Dunkels (2010), salientando que usuários com maior grau de instrução tendem a facilitar a implantação unificada do ambiente inteligente por conseguirem utilizar diversos tipos dispositivos sem prejuízos a experiência de uso.

Partindo dessa característica pode-se traçar um perfil dos usuários, como exposto no quadro 6 a seguir, os usuários em relação ao gênero estão equilibrados, com uma leve predominância aos usuários do gênero masculino, são em sua maioria jovens abaixo dos 30 anos e com grau de escolaridade mediano.

**Quadro 6:** Perfil dos usuários respondentes da pesquisa

<b>Característica Analisada</b>	<b>Perfil encontrado</b>
<b>Gênero</b>	Equilíbrio entre gêneros com 41,92% feminino e 57,64% masculino.
<b>Faixa etária</b>	58,95% possuem até 30 anos.
<b>Grau de escolaridade</b>	57,64% possuem ensino médio concluído ou um grau de instrução acima.

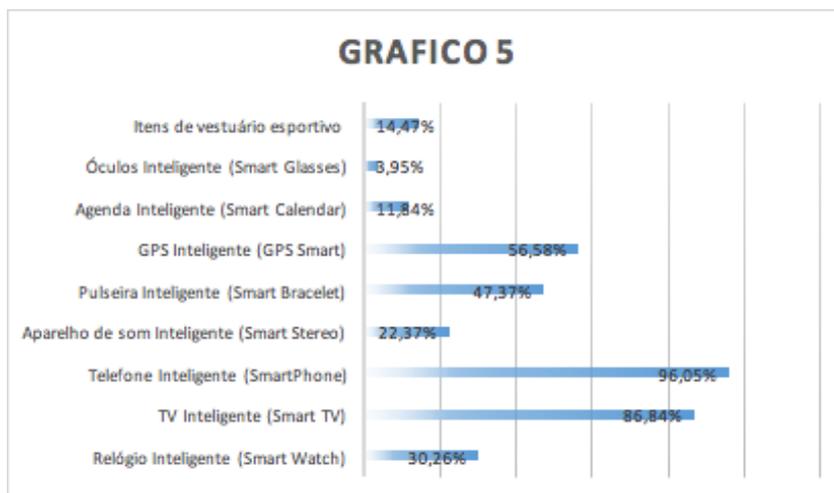
Fonte: Dados da pesquisa (2016).

Traçar este perfil torna-se parte essencial da pesquisa, para melhor compreender as preferências e as escolhas realizadas pelos usuários, como os tipos de tecnologias por eles utilizadas, que serão apresentados na seção a seguir. Neste sentido admite-se que as escolhas e comportamentos encontrados neste estudo tem maior predominância para este perfil de usuário.

#### 4.2 Tipos de tecnologias inteligentes

Objetivando identificar os tipos de tecnologias inteligentes utilizadas pelos usuários, já que este é um dos propósitos desta investigação, foram aplicadas as perguntas dos itens 5 a 7 que buscaram verificar informações pertinentes quanto a posse e a utilização dos dispositivos.

Dessa forma, os dados da pesquisa apontaram que os dispositivos de tecnologia inteligente mais populares possuídos pelos respondentes da pesquisa, como apresentado pelo gráfico 5, são os *smartphones* e as *smart TVs* com 96,05% e 86,84% dos respondentes declarando possuir um desses dispositivos, respectivamente.

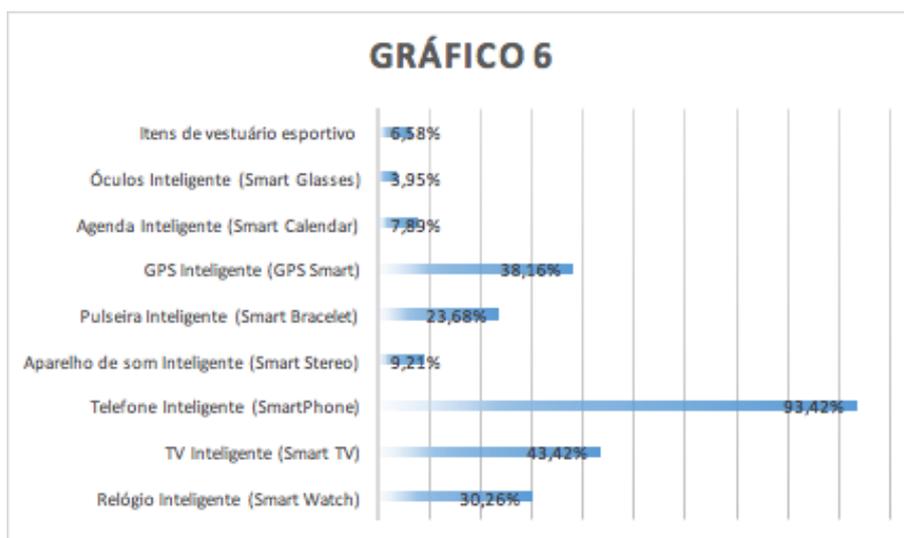
**Gráfico 5: Dispositivos Inteligentes**

Fonte: Dados da Pesquisa (2016).

O que chama atenção entre os dispositivos inteligentes listados acima são os itens de vestuário, apesar de pouco difundidos no país até o momento deste estudo, 14,47% dos respondentes afirmam possuir algum dispositivo dessa natureza. Assim como os 3,95% dos respondentes que já declaram possuir óculos inteligente.

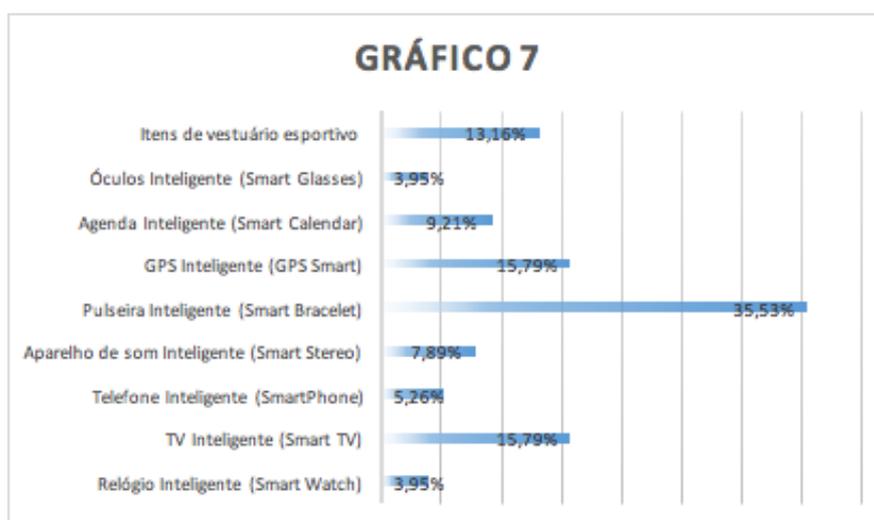
Em seu uso diário o *smartphone*, como já identificado na pesquisa de Li, Da Xu e Zhao (2014), é o dispositivo mais utilizado pelos respondentes, o que corrobora também com Chabrindon (2014) que menciona que este artefato se torna um dispositivo indispensável na implementação de soluções inteligentes. Tal como esperado por Atzori, Iera e Morabito (2010) que relaciona a evolução do uso de aparelhos celulares com a evolução das tecnologias IoT baseada na necessidade de comunicação integrada e contínua.

O que se evidencia no gráfico 6, é que mesmo sendo a *smart TV* um dispositivo utilizado por 86,84% dos respondentes, destes apenas 40,8% fazem uso dos dispositivos diariamente, representando menos da metade dos respondentes que declararam possuir o dispositivo. Esta realidade torna-se ainda mais evidente quando confrontada com o gráfico 7, Dispositivos em desuso, em que 15,79% dos respondentes declaram possuir uma *smart TV*, mas mantém o dispositivo em desuso.

**Gráfico 6:** Uso diário de dispositivos inteligentes

Fonte: Dados da Pesquisa (2016).

Entretanto, a presença da *smart TV* nas residências, mesmo que fora de seu uso diário, configura-se como uma oportunidade, visto que, para autores como Miorandi *et al.* (2012) e Brody e Pureswaran (2015) dispositivos inteligentes presentes dentro de casa e de uso coletivo, são essenciais para o desenvolvimento de ambientes inteligentes de uso doméstico e para a difusão do conceito de casa inteligente.

**Gráfico 7:** Dispositivos em desuso

Fonte: Dados da Pesquisa (2016).

Em comparação com o alto índice de uso do *smartphone* observa-se também a queda do uso de GPS e das agendas inteligentes, situação que tende a se elevar visto que o *smartphone* desfralda a substituir as funções desempenhadas por estes dispositivos. Contudo a pulseira inteligente é o dispositivo que mais chama atenção pelo desuso, pois 35,53% dos respondentes que declararam possuir o dispositivo o mantém em desuso, levando em consideração que o índice de desuso do relógio inteligente foi de 3,95% e que este tipo de dispositivo comumente possui funcionalidades que podem substituir as pulseiras inteligentes, este pode ser considerado uma das causas do acentuado desuso desse dispositivo.

O declínio do uso de dispositivos em detrimento da adoção de outros que agreguem novas e antigas funções é uma tendência já observada pela indústria e já relatada pelos estudos de Floerkemeier, Roduner e Lampe (2007) e Domingo (2012) que sinalizam a necessidade contínua das novas tecnologias se fundirem e agregarem diversas funcionalidades a fim de criarem um ambiente capaz de lidar com a diversidade de tarefas e com o surgimento de novas soluções.

Com base nos dados expostos, os tipos de tecnologias inteligentes encontradas em campo possuem considerável variedade, ainda que não seja identificado uso em massa dessas tecnologias. Observando maior predominância do uso do *smartphone*, como apresentado a seguir pelo quadro 7, que expõem o resumo dos dados encontrados em relação aos tipos de tecnologias e sua frequência de uso pelos usuários.

**Quadro 7:** Tipos de tecnologias inteligentes

<b>Característica Analisada</b>	<b>Tipo de tecnologia inteligente encontrada</b>
<b>Dispositivos inteligentes mais populares</b>	<i>Smartphones</i> 96,05% e as <i>smart TVs</i> 86,84%
<b>Dispositivo mais utilizado diariamente</b>	<i>Smartphones</i> 93,47%
<b>Dispositivo mais mantido em desuso</b>	Pulseira inteligente 35,53%

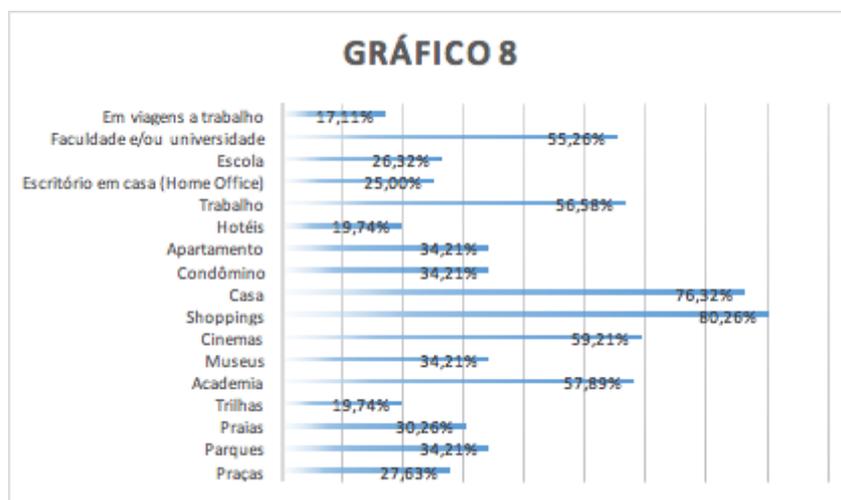
Fonte: Dados da pesquisa (2016).

### 4.3 Ambiente de uso dos dispositivos e principais finalidades

Com o objetivo de descrever as formas de uso cotidiano das tecnologias inteligentes, foram realizadas as perguntas dos itens 8 a 12 buscando verificar ambientes comuns de uso para os usuários e principais finalidades de uso dos dispositivos inteligentes.

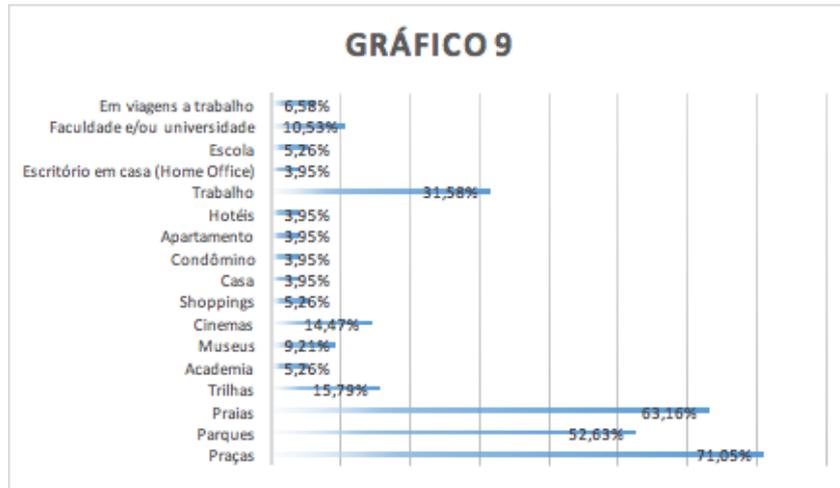
Desse modo, observou-se por meio dos dados da pesquisa que o uso dos dispositivos inteligentes, como apresentado pelo gráfico 8, torna-se mais acentuado em locais de uso comum e fechado, como na academia (57,89%), em casa (76,32%), no shopping (80,26%) e na faculdade (55,26%). No entanto, esse uso se reduz de forma acentuada em relação a ambientes abertos como praças (27,63%) e parques (34,21%), essa redução reflete em questões já levantadas por Meirelles (2014) em relação a qualidade da conexão móvel e do acesso a internet em locais públicos, assim com a segurança pública para a utilização de determinados dispositivos em locais abertos.

**Gráfico 8:** Ambientes de uso



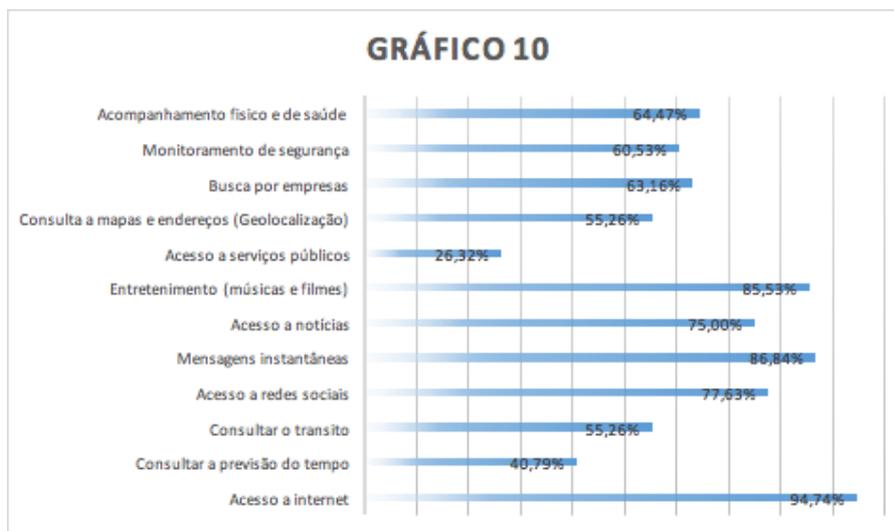
Fonte: Dados da Pesquisa (2016).

Situação que é reforçada em comparação com o gráfico 9 que vem logo adiante, em que 71,05% dos respondentes afirmaram evitar utilizar seus dispositivos em praças e 63,16% em praias.

**Gráfico 9:** Ambientes de uso evitados

Fonte: Dados da Pesquisa (2016).

Destaca-se também que, apesar da inegável utilidade das tecnologias inteligentes, tais dispositivos ainda não foram absorvidos e postos à disposição pelos setores públicos a fim de melhorar seus serviços e produtos, como evidenciado no gráfico 10, ter acesso a serviços públicos é a finalidade de uso menos utilizada pelos usuários. Este fenômeno, no entanto, não é exclusivo do Brasil, visto que Atzori, Iera e Morabito (2010) já destacaram esta realidade em seu estudo realizado em outros cenários.

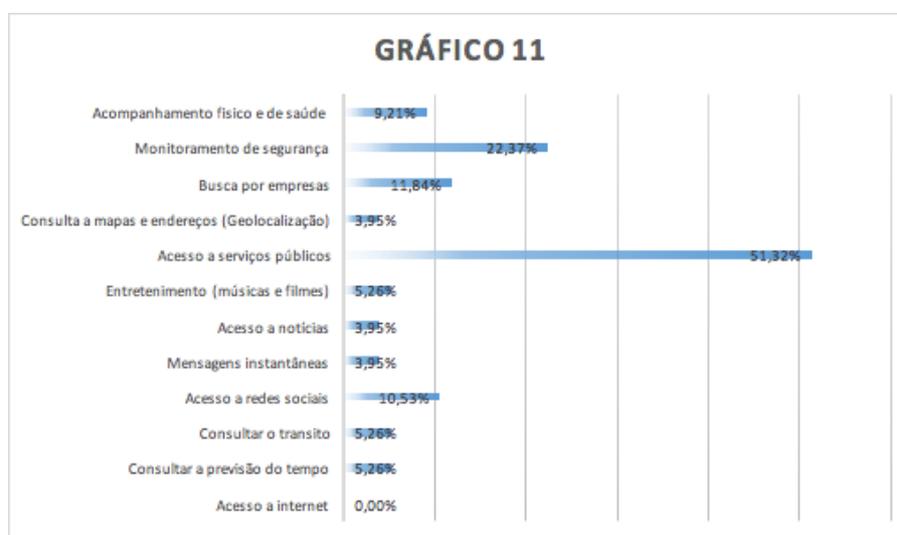
**Gráfico 10:** Finalidades de uso dos dispositivos

Fonte: Dados da Pesquisa (2016).

Dentro dessa realidade, ao questionar para quais finalidades os usuários evitavam utilizar seus dispositivos inteligentes, foi possível confirmar, como apresentado no gráfico 11, um maior destaque aos serviços públicos, onde 51,32% dos respondentes sinalizaram evitar esse tipo de uso. O que evidencia a baixa disposição dos usuários em realizar serviços públicos por meio de seus dispositivos inteligentes, fenômeno que já previsto por Zorzi (2010) que ao afirmar que as tecnologias IoT possuem potencial de melhorar a qualidade de vida das pessoas já alertava que o fornecimento de serviços avançados por parte do setor público dependeria não apenas de infraestrutura tecnológica, mas da iniciativa da população de aceitar tais mudanças e utilizar as novas soluções.

Em contraponto, Saxby (2015) atribui aos gestores públicos a responsabilidade de despertar no usuário a aceitação de tais serviços por estes meios, afirmando que para alcançar a realidade de cidade inteligente é necessário dedicar maior atenção, não apenas a implantação de tecnologias inteligentes, mas também a aceitação e ao uso dessas tecnologias pelos usuários.

**Gráfico 11:** Finalidades de uso evitadas pelos usuários

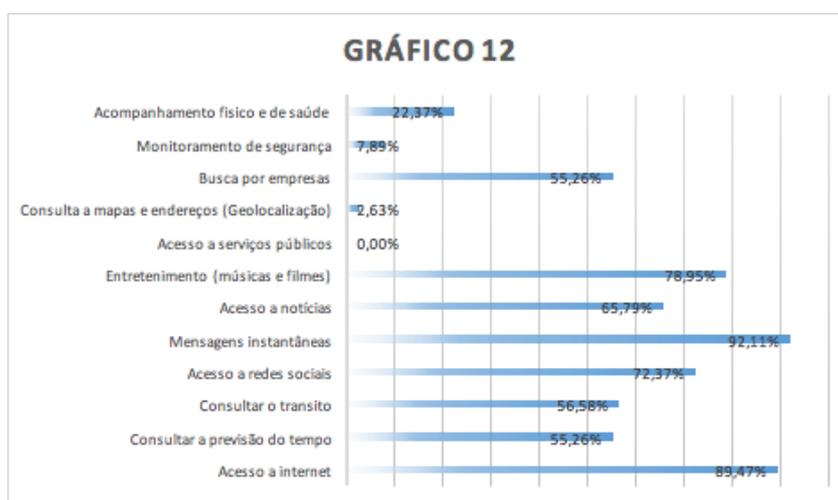


Fonte: Dados da Pesquisa (2016).

Ao se questionar quais as três principais finalidades de uso dos dispositivos, pode-se constatar que não obstante a pesquisa realizada por Botterman (2009), mensagens instantâneas, acesso a internet e entretenimento são os principais

usos dos dispositivos inteligentes, reflexo também do dispositivo inteligente mais utilizado ser o *smartphone*.

**Gráfico 12:** Três principais finalidades de uso dos dispositivos



Fonte: Dados da Pesquisa (2016).

Contudo destaca-se que no mercado brasileiro, assim como já identificado por Cusumano e Goeldi (2013) e Brody e Pureswaran (2015) em outros mercados, existe um cenário promissor para empresas em outros setores, visto que, como apresentado no gráfico 12, busca por empresas é uma das três principais razões de uso em 55,26% dos casos, o que pode ser visto como uma oportunidade de explorar produtos e serviços por meio dessas tecnologias.

Os dados da pesquisa apresentados em relação aos ambientes de uso e principais finalidades escolhidas pelos usuários são resumidos e apresentados no quadro 8, com o objetivo de melhor apresentar os achados identificados.

**Quadro 8:** Ambiente de uso e principais finalidades

Característica Analisada	Ambiente de uso e principais finalidades
<b>Ambiente de uso mais utilizados</b>	Locais de uso comum e fechado: Academia, casa, shopping e faculdade
<b>Ambientes de uso mais evitados</b>	Locais abertos: Praças, parques
<b>Finalidade de uso dos dispositivos</b>	Acesso a internet, mensagens instantâneas e entretenimento
<b>Finalidade de uso mais evitada</b>	Acesso a serviços públicos

Fonte: Dados da Pesquisa (2016).

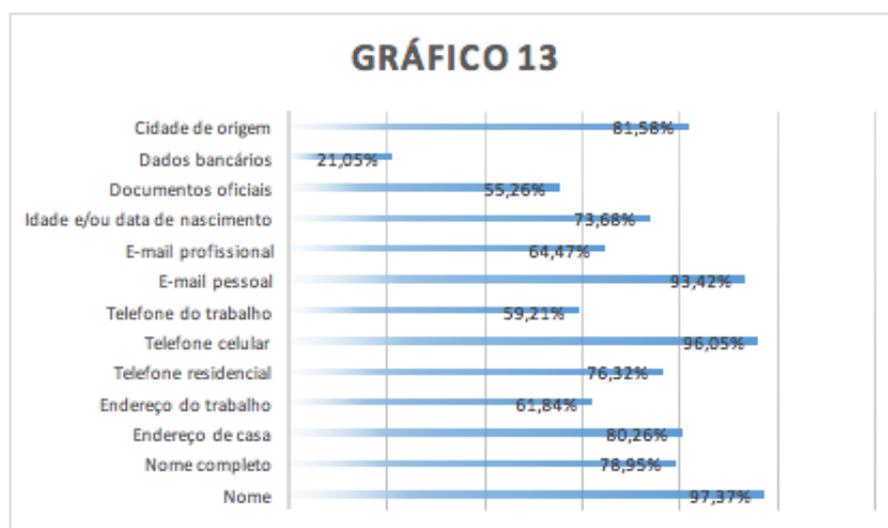
A compreensão do comportamento do usuário perpassa pela identificação e caracterização dos locais por eles frequentados, observar quais locais predominam entre a amostra estudada está condicionado a um melhor entendimento dos dados e informações que são disponibilizados por meio dos dispositivos inteligentes, dados estes que serão analisados a seguir.

#### 4.4 Dados e informações disponibilizados por meio dos dispositivos

Almejando identificar os tipos de dados e informações fornecidos em ambientes inteligentes, foram realizadas as perguntas dos itens 13 a 16 buscando levantar quais dados e informações são disponibilizados por meio desses dispositivos.

Ao quesito quais dados pessoais os usuários disponibilizam em seus dispositivos, destacou-se a preocupação dos usuários em relação a segurança de seus dados bancários, como pode ser verificado no gráfico 13, em que apenas 21,05% dos respondentes declaram disponibilizar seus dados bancários por meio de dispositivos inteligentes.

**Gráfico 13:** Dados e informações disponibilizados



Fonte: Dados da Pesquisa (2016).

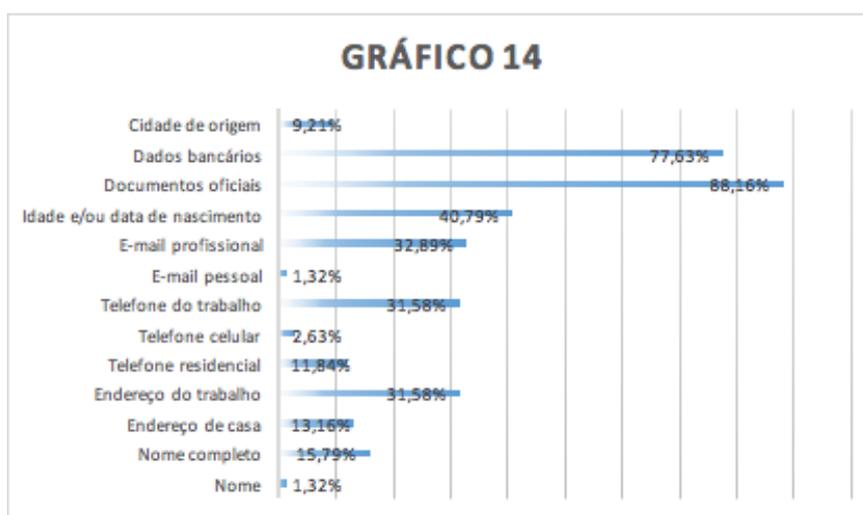
Este resultado deve ser visto com atenção, não apenas pelo setor bancário, visto que produtos e serviços de diversas naturezas podem ter suas oportunidades de

negócios reduzidas pela recusa dos usuários em disponibilizar seus dados bancários por meio de dispositivos inteligentes.

Situação esta que se reforça ao questionar quais dados pessoais os usuários evitam disponibilizar em seus dispositivos, como exposto no gráfico 14, em que os dados bancários são assinalados por 77,63% dos entrevistados como um dado que eles evitam disponibilizar, assim como documentos oficiais que 88,16% dos entrevistados afirmaram evitar disponibilizar em seus dispositivos inteligentes. Corroborando com esses resultados estão as afirmações de Berners-Lee e O'Hara (2013) ao afirmarem que as ações capazes de alavancar o uso das tecnologias IoT no mercado financeiro e em esferas governamentais ainda são demasiadas insuficientes. Tal com para Li, Da Xu e Zhao (2014) ao demonstrar a preocupação dos usuários para com dados de teor financeiro e documentos importantes, trazendo a tona a preocupação dos usuários com a privacidade dentro dos ambientes inteligentes.

Assim como os estudos de Atori, Iera e Morabito (2010) e Miorandi et al. (2012) Ashraf e Habaebi (2015), ao tratar de aplicações de negócios, já destacam em seus estudos que devido a sensação de insegurança e falta de privacidade presente no ambiente inteligente, empresas e usuários mantêm soluções inteligentes como soluções secundárias na empresa, resistindo ao uso primário.

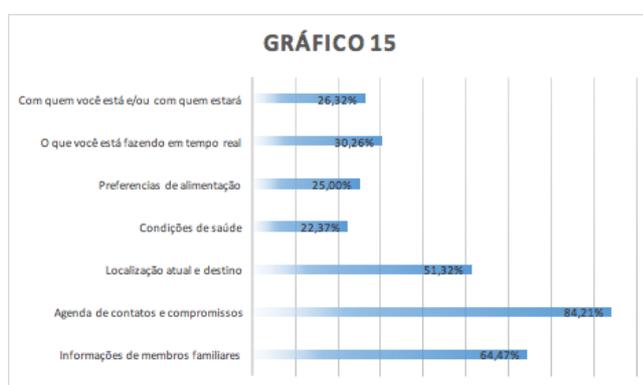
**Gráfico 14:** Dados e informações que evitasse disponibilizar



Fonte: Dados da Pesquisa (2016).

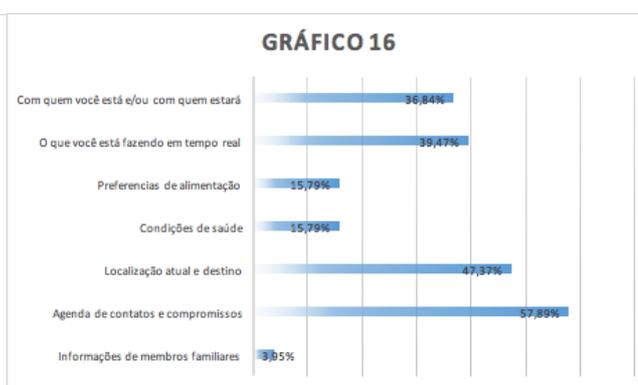
Buscando verificar se haveria diferenças no comportamento do usuário em relação as informações disponibilizadas por meio dos dispositivos inteligentes, questionou-se quais informações eram fornecidas com frequência em seus dispositivos em uso doméstico, como apresentado no gráfico 15, e em uso profissional, como apresentado no gráfico 16.

**Gráfico 15:** Dados e informações disponibilizados em uso doméstico



Fonte: Dados da Pesquisa (2016).

**Gráfico 16:** Dados e informações disponibilizados em uso profissional



Fonte: Dados da Pesquisa (2016).

O comparativo dos dados leva a crer que informações como agenda de contatos e compromissos, localização atual e destino, condições de saúde e preferência de alimentação, são informações disponibilizadas de maneira semelhante em dispositivos de uso doméstico e profissional.

Contudo informações de membros familiares que em dispositivos de uso domésticos são amplamente fornecidas, alcançando 64,47% dos usuários, em dispositivos profissionais os usuários evitam disponibilizar informações dessa natureza, visto que apenas 3,95% dos respondentes sinalizaram disponibilizar esse tipo de informação em dispositivos inteligentes em uso profissional.

Observou-se também que informações que envolvem outras pessoas (do tipo: com quem o usuário está e com quem ele estará) são disponibilizadas com maior frequência em dispositivos que estão em uso profissional, tal situação é motivada por exigências das empresas empregadoras que necessitam acompanhar as atividades dos profissionais, como evidenciado por Weber (2010) que destaca o potencial da IoT para atividades que necessitem de acompanhamento remoto. No entanto, levando

em consideração que tal monitoramento pode ser considerado um abuso da privacidade do usuário quando mantido fora do horário de trabalho, Solove (2006) argumenta que o uso doméstico e o uso profissional de dispositivos inteligentes devem ser tratados de forma isolada. Contrários a essa ideia Cusumano e Goeldi (2013) e Brody e Pureswaran (2015) ressaltam a necessidade de criar soluções universais, pois a fragmentação das tecnologias IoT podem dificultar a implantação de soluções e inviabilizar a criação de um ambiente inteligente unificado.

O fenômeno aqui identificado, vem em contraponto ao posicionamento de Solove (2006) incrementando as ideias de Cusumano e Goeldi (2013) e Brody e Pureswaran (2015) partindo de uma nova perspectiva, em que não se torna necessário, por parte da indústria, preocupar-se com quais soluções serão disponibilizadas para quais tipos de atividades, visto que o usuário tende a comportar-se de forma diferente em ambientes distintos, dando também usos distintos aos dispositivos inteligentes que estão em uso.

A seguir o quadro 9 resume o que foi apresentado a respeito dos dados e informações que são disponibilizados por meio de dispositivos inteligentes, buscando em síntese apresentar quais foram as predominâncias em relação a amostra estudada.

**Quadro 9: Dados e informações disponibilizados por meio dos dispositivos**

<b>Característica Analisada</b>	<b>Dados e informações disponibilizados</b>
<b>Dados e informações disponibilizadas em ambos os ambientes</b>	Agenda de contatos e compromissos, localização atual e destino, condições de saúde e preferência de alimentação
<b>Dados e informações disponibilizadas em uso doméstico</b>	Informações de membros familiares
<b>Dados e informações disponibilizadas em uso profissional</b>	Quem o usuário está e com quem ele estará
<b>Dados e informações que se evita disponibilizar</b>	Dados bancários e documentos oficiais

Fonte: Dados da Pesquisa (2016).

Essas predominâncias são de vital importância para a compreensão do fenômeno em tela, visto que, ao definir que tipo de dado e de informação são mais recorrentes no estudo, observa-se que possíveis aspectos considerados predominantes pelos usuários para o fornecimento de seus dados e informações deverão ter sua relevância observada predominantemente para esses tipos de

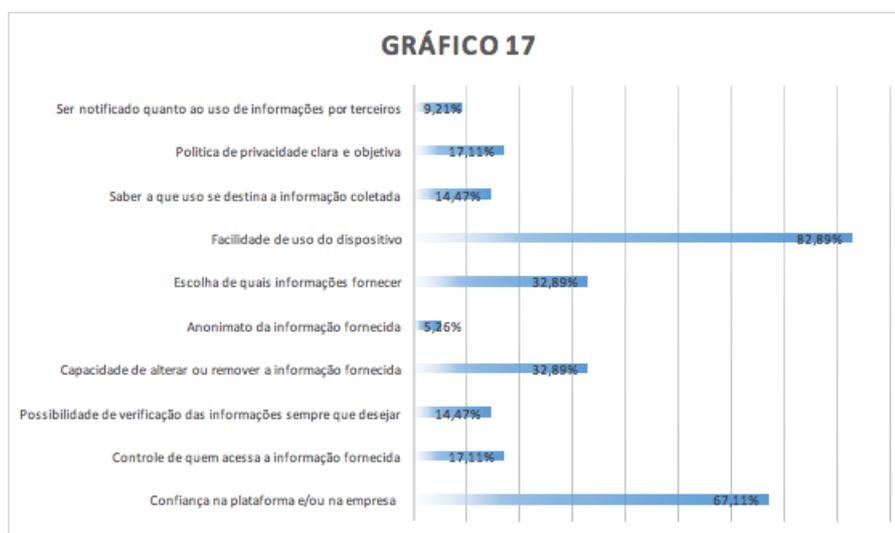
informações, visto que se torna necessário creditar os aspectos encontrados ao tipo de informação fornecida.

#### 4.5 Aspectos determinantes para o fornecimento de dados e informações

Com o objetivo de analisar os aspectos determinantes para o fornecimento de dados e informações no ambiente inteligente, foram aplicadas as perguntas dos itens 17 e 18, com as quais buscou-se as condições percebidas pelos usuários como determinantes ao fornecimento de suas informações pessoais.

Identificou-se em âmbito doméstico que, como pode ser observado no gráfico 17, a facilidade de uso do dispositivo é o maior fator levado em consideração pelos usuários para disponibilizar suas informações, representando 82,89%. Logo, acredita-se que dispositivos com usabilidade facilitada para o usuário final, tendem a receber um volume maior de informações em detrimento de dispositivos que tenham maior preocupação com a segurança da informação e da privacidade do usuário.

**Gráfico 17:** Aspectos determinantes para o fornecimento de dados e informações em ambiente doméstico



Fonte: Dados da Pesquisa (2016).

Este achado corrobora com as afirmações de Welbourne (2009) ao ponderar que a implementação de tecnologias inteligentes necessitaria de um alto nível de padronização para garantir operabilidade, mas que tais investimentos precisam estar alinhados com a experiência de uso e expectativas do usuário, visto

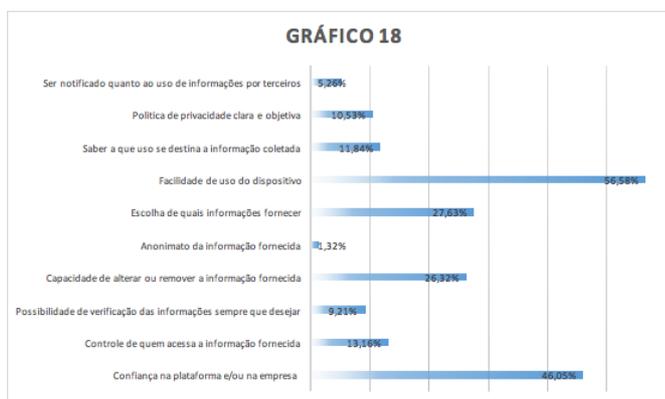
que a preocupação com a privacidade por parte do fornecedor da solução não é facilmente percebida pelo usuário. Neste sentido, espera-se encontrar um equilíbrio entre a privacidade do usuário a facilidade de uso do dispositivo, como sugere o autor.

Observou-se também que o usuário em atitude doméstica transpõe para a empresa responsável pelo dispositivo e/ou pela plataforma ao qual está conectado a sua confiança e subsequente responsabilidade em salvaguardar a sua privacidade, tendo neste fator uma predominância de 67,11% dos respondentes que consideram esta uma condição predominante para o fornecimento de informações. Esse comportamento de transposição de confiança identificado nos usuários justifica-se pela confiança preestabelecida na relação de consumo entre o usuário e a empresa prestadora da solução e no pouco conhecimento técnico por vezes necessário para compreender outros fatores investigados como a política de privacidade adotada pela empresa responsável, assim como o incomodo gerado por notificações de uso de terceiros.

Contudo vale ressaltar que esse comportamento de transposição de confiança dificilmente será alterado a curto prazo como afirmam Kranz, Roalter e Michahelles (2010) ao considerarem pouco provável uma mudança no comportamento do usuário apenas pela conscientização do risco a sua privacidade. Em observância disto, recomenda-se que este aspecto seja explorado de outra maneira, utilizando essa predisposição do usuário na construção de padrões para oferta de soluções mais aprimoradas e para o estabelecimento de um padrão de consumo que possa ser melhor explorado, passando a pensar a transposição de confiança como um padrão de apoio a implementação da IoT a ser explorado (CUSUMANO; GOELDI, 2013, BRODY; PURESWARAN, 2015).

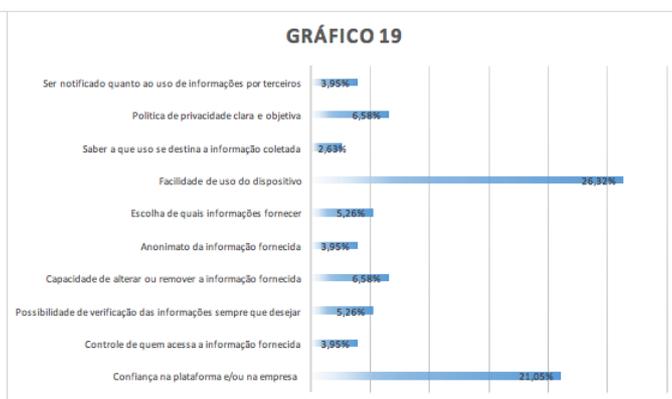
Quando realizado um extrato por gênero, comparando o gráfico 18, condições que determinam o fornecimento de informações para usuários do gênero masculino, e o gráfico 19, condições que determinam o fornecimento de informações para usuários do gênero feminino, pode-se observar que os usuários do gênero feminino possuem uma maior preocupação com a capacidade de escolha de qual informação fornecer, do que os usuários do gênero masculino deferindo em percentual de 27,63% para 5,26% respectivamente.

**Gráfico 18:** Condições que determinam o fornecimento de informações para usuários do gênero masculino



Fonte: Dados da Pesquisa (2016).

**Gráfico 19:** Condições que determinam o fornecimento de informações para usuários do gênero feminino



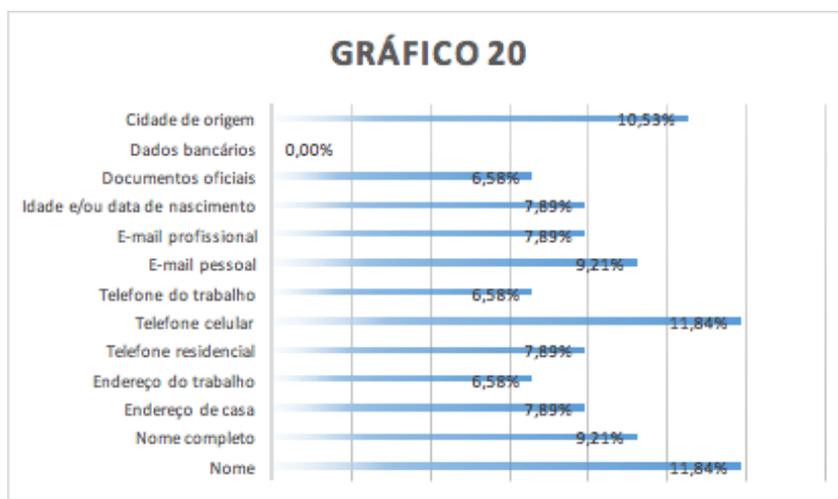
Fonte: Dados da Pesquisa (2016).

Distinção semelhante também foi identificada para a capacidade de alterar ou remover a informação fornecida, que para os usuários de gênero feminino possuem uma maior relevância do que para os usuários de gênero masculino, apresentando uma relevância de 26,32% e 6,58% respectivamente. No entanto ao confrontar esses resultados estratificando-os por faixa etária, por região do país e por escolaridade não foram encontradas diferenças relevantes, indicando que tais variáveis não impactam na percepção dos respondentes aos fatores determinantes para fornecimento de informações.

Sendo a facilidade de uso do dispositivo e a confiança na plataforma e/ou empresa as condições principais para o fornecimento de informações escolhida pelos usuários respondentes da pesquisa, confrontou-se o resultado dos tipos de dados fornecidos pelos usuários isolando essas variáveis, isoladamente estas não apresentam nenhuma influencia sobre as demais. No entanto, juntas, como exposto no gráfico 20, pode-se constatar que houve redução percentual para zero dos usuários que disponibilizam seus dados bancários, mas não há discrepância percentual considerável nos outros tipos de dados disponibilizados, isso leva a crer que mesmo se tratando de duas condições determinantes para o fornecimento de dados por meio do dispositivo inteligente, estas condições por si só não influenciam na escolha dos

dados que serão disponibilizados, entretanto são indispensáveis para usuários que desejem disponibilizar dados de natureza financeira.

**Gráfico 20:** Condições principais para o fornecimento de informações



Fonte: Dados da Pesquisa (2016).

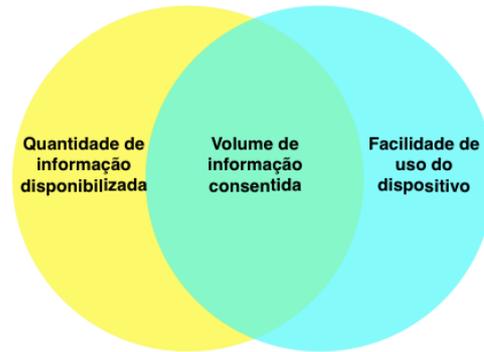
Ao confrontar essas duas variáveis com os tipos de informações que são fornecidas no ambiente inteligente, a condição de facilidade de uso, não demonstrou influenciar percentualmente os tipos de informação que são fornecidas, constata-se que ela é capaz de influenciar apenas a quantidade de informação que é disponibilizado, no entanto parece ser incapaz de influenciar nos tipos de informações que serão disponibilizadas no ambiente inteligente.

Tal constatação torna esse fator influente na quantidade de informação que pode ser disponibilizada pelo usuário, podendo encontrar semelhanças na taxonomia definida por Solove (2006) a respeito da capacidade de coleta de informações, baseada no consentimento do usuário.

Sendo assim, a informação consentida pelo usuário posiciona-se nas linhas de fronteiras pessoais, definidas por Marx (2001) como fronteira natural a que define obstáculos naturais a observação ou a disseminação da informação influenciando a percepção de privacidade do usuário. Tendo o fenômeno encontrado um conjunto de elementos constituídos de características dos dois posicionamentos teóricos nos quais tratam da quantidade de informação disponibilizada e do seu consentimento em detrimento da privacidade do usuário, afirma-se que o volume de informação

consentida, depende da relação entre a quantidade de informação disponibilizada e a facilidade de uso do dispositivo utilizado, como ilustrado na figura 5.

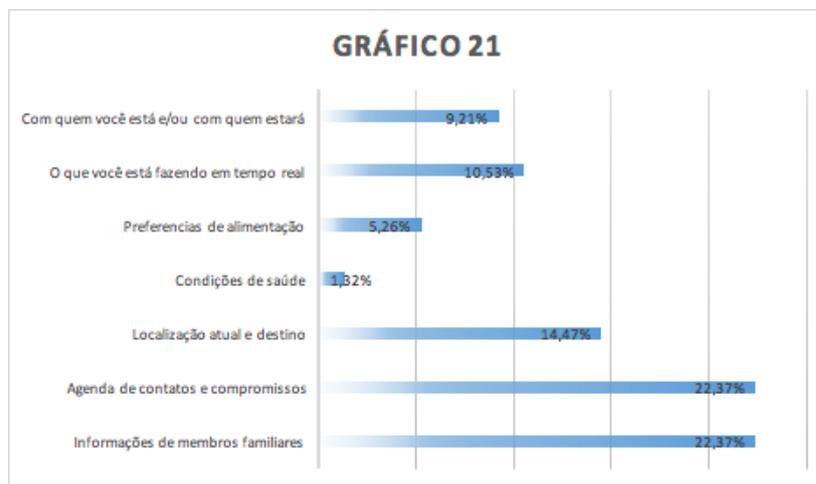
**Figura 5:** Volume de informação consentida



Fonte: Elaborado pelo autor (2016).

Em contrapartida, a condição de confiança na plataforma e/ou empresa, como apresentado no gráfico 21, influenciou de maneira significativa nas condições de informações de preferência de alimentação, condições de saúde e informações de membros familiares, revelando que a confiança na plataforma pode influenciar de maneira mais significativa a escolha das informações de natureza individuais, no entanto as informações de naturezas sociais, não são igualmente influenciadas por esta condição.

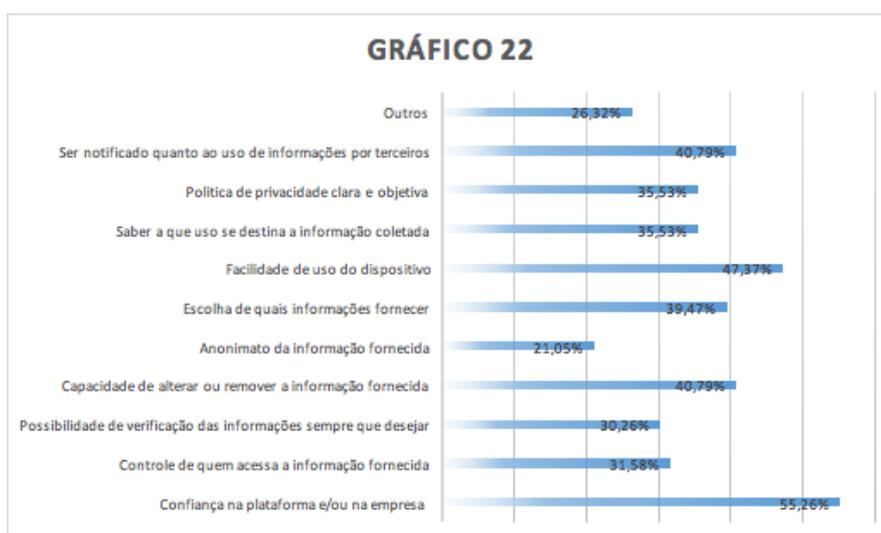
**Gráfico 21:** Tipos de informações que são fornecidas no ambiente inteligente em relação a condição de facilidade de uso do dispositivo inteligente



Fonte: Dados da Pesquisa (2016).

Quando solicitado que os respondentes da pesquisa assinalassem as condições que determinavam o fornecimento de informações em seus dispositivos inteligentes em ambientes profissionais, os resultados encontrados divergiram dos encontrados em ambientes domésticos, como pode ser observado no gráfico 22, os fatores vistos como determinantes pelos usuários em ambientes profissionais são mais equilibrados entre si, mantendo a confiança na plataforma (55,26%) e facilidade de uso (47,37%) como os fatores mais observados, no entanto fatores como ser notificado quanto ao uso de informações por terceiros (40,79%), capacidade de alterar ou remover a informação fornecida (40,79%) e escolha de quais informações fornecer (39,47%) ganham considerável importância diante dos demais fatores.

**Gráfico 22:** Aspectos determinantes para o fornecimento de dados e informações em ambiente profissional



Fonte: Dados da Pesquisa (2016).

O equilíbrio entre os fatores apresentados no ambiente profissional, atribui-se ao fator outros, fator que descreve em sua maioria o auxílio de um profissional especializado para a escolha mais apropriada a ser utilizada na empresa por meio da análise dos outros fatores, tal qual como relatado pelos respondentes e observado de forma percentual como ele influencia diretamente nos demais fatores.

Partindo das linhas de fronteiras pessoais definidas por Marx (2001) tal comportamento pode ser enquadrado na fronteira social, tendo em vista que os

usuários transferiram a responsabilidade de tomar decisões que possam garantir a sua privacidade dentro da empresa para um profissional especializado no qual se deposita expectativa de confiança em cuidar de seus dados.

No entanto, como defendem autores como Krause (2009) e Chabridon *et al.* (2014), delegar decisões que dizem respeito a manutenção da privacidade a terceiros podem acarretar em risco à própria essência da privacidade. Neste sentido, credita-se esta preocupação ao fenômeno aqui encontrado, tendo em vista que quando é dado ao usuário maior liberdade de escolha em seu ambiente doméstico, este não utiliza os mesmos critérios que é orientado a utilizar por profissionais especializados no ambiente profissional, buscando critérios mais simplificados e de fácil compreensão, caracterizando desta forma a busca pela simplificação dos critérios de manutenção da privacidade.

**Quadro 10: Aspectos determinantes para o fornecimento de dados e informações**

<b>Característica Analisada</b>	<b>Aspectos determinantes</b>
<b>Aspectos determinantes em ambiente doméstico</b>	Facilidade de uso do dispositivo; confiança na plataforma e/ou na empresa responsável
<b>Aspectos determinantes em ambiente profissional</b>	Orientação de profissionais especializados proporcionam equilíbrio entre os aspectos analisados

Fonte: Dados da Pesquisa (2016).

Os aspectos determinantes predominantes entre os usuários participantes da pesquisa, estão resumidos no quadro 10, mostrado acima. Identificar estes aspectos é condição necessária para se compreender as especificidades entre o ambiente doméstico e profissional por meio da categorização do que é predominante em cada tipo de ambiente.

#### 4.5 Resultados predominantes achados em campo

Para melhor visualizar os achados de cada etapa da pesquisa abordado até aqui, o quadro 11 apresenta em resumo as características analisadas, destacando as predominâncias identificadas nos dados coletados em campo. Observar essas predominâncias de maneira conjunta e sequenciada auxilia na compreensão dos principais achados atribuídos a estes dados.

**Quadro 11:** Resultados predominantes encontrados em campo

<b>Característica Analisada</b>	<b>Resultado predominante</b>
<b>Dispositivos inteligentes mais populares</b>	<i>Smartphones 96,05% e as smart TVs 86,84%</i>
<b>Dispositivo mais utilizado diariamente</b>	<i>Smartphones 93,47%</i>
<b>Dispositivo mais mantido em desuso</b>	Pulseira inteligente 35,53%
<b>Ambiente de uso mais utilizados</b>	Locais de uso comum e fechado: Academia, casa, shopping e faculdade
<b>Ambientes de uso mais evitados</b>	Locais abertos: Praças e parques
<b>Finalidade de uso dos dispositivos</b>	Acesso a internet, Mensagens instantâneas e entretenimento
<b>Finalidade de uso mais evitada</b>	Acesso a serviços públicos
<b>Dados e informações disponibilizadas em ambos os ambientes</b>	Agenda de contatos e compromissos, localização atual e destino, condições de saúde e preferência de alimentação
<b>Dados e informações disponibilizadas em uso doméstico</b>	Informações de membros familiares
<b>Dados e informações disponibilizadas em uso profissional</b>	Com quem o usuário está e com quem ele estará
<b>Dados e informações que se evita disponibilizar</b>	Dados bancários e documentos oficiais
<b>Aspectos determinantes em ambiente doméstico</b>	Facilidade de uso do dispositivo; confiança na plataforma e/ou na empresa responsável
<b>Aspectos determinantes em ambiente profissional</b>	Orientação de profissionais especializados proporcionam equilíbrio entre os aspectos analisados

Fonte: Dados da Pesquisa (2016).

Com o objetivo de esquematizar os principais achados em campo, a figura 6 destaca os aspectos determinantes para o fornecimento de informações pessoais em ambientes inteligentes, podendo estes serem interpretados dentro do contexto amplo do ambiente inteligente.

1) O ambiente de uso é apresentado como aspecto que contempla continuamente os outros, por ser capaz de influenciar a disponibilização de informações no ambiente inteligente, como também a maneira como os outros aspectos são percebidos pelos usuários. A definição da natureza do ambiente ao qual a tecnologia IoT está sendo aplicada torna-se passo essencial para a compreensão dos outros aspectos determinantes, contribuindo para minimizar a

preocupação destacada por Solove (2006) a respeito da fragmentação da tecnologia, possibilitando a geração de um ambiente inteligente de uso único.

A compreensão da natureza do ambiente de uso pode incrementar as ideias de Cusumano e Goeldi (2013) e Brody e Pureswaran (2015) partindo de uma nova perspectiva, em que não se torna necessário por parte da indústria preocupar-se em quais soluções serão disponibilizadas para quais tipos de atividades, visto que foi observado que o usuário tende a comportasse de forma diferente em ambientes distintos, dando também usos distintos aos dispositivos inteligentes e fornecendo informações distintas. Nesse contexto compreender a natureza do ambiente de uso torna possível a adoção de uma determinada tecnologia para variadas realidades deixando a personalização a cargo dos usuários, que a fará de acordo com a sua percepção de necessidade;

2) A transposição de confiança é observada quando o usuário transfere para a empresa responsável pelo dispositivo e/ou pela plataforma ao qual está conectado a sua confiança e subsequente responsabilidade em salvaguardar a privacidade do usuário. Neste sentido, como defende Marx (2001) o usuário passa para um terceiro a sua confiança e conseqüentemente suas informações com maior facilidade, logo a compreensão desse aspecto pode torna-se determinante para a popularização das tecnologias IoT, baseado na confiança de marcas e empresas por elas responsáveis, assim como recomenda de Cusumano e Goeldi (2013) e Brody e Pureswaran (2015) para que, uma vez identificado um padrão emergente de apoio a implementação da IoT, seja explorado como parte integrante do todo;

3) O volume de informação consentida diz respeito à relação entre a quantidade de informação a ser disponibilizada e a facilidade de uso do dispositivo utilizado. Esta relação encontra semelhanças na taxonomia definida por Solove (2006) a respeito da capacidade de coleta de informações, baseada no consentimento do usuário e posicionando-se nas linhas de fronteiras pessoais definidas por Marx (2001) como fronteira natural, a que define obstáculos naturais a observação ou a disseminação da informação influenciando a percepção de privacidade do usuário.

Sendo encontrado no volume de informação consentida um conjunto de elementos constituídos de características dos dois posicionamentos teóricos nos quais tratam do volume de informação disponibilizada e do seu consentimento em detrimento da privacidade do usuário, afirma-se que o volume de informação

consentida depende da relação entre a quantidade de informação disponibilizada e a facilidade de uso do dispositivo utilizado. Partindo dessa afirmação acredita-se que este aspecto possui potencial determinante para reduzir ou elevar o volume de informação que o usuário se propõe a disponibilizar, tornando-se estratégico para soluções que necessitem de um maior volume de informações para funcionar;

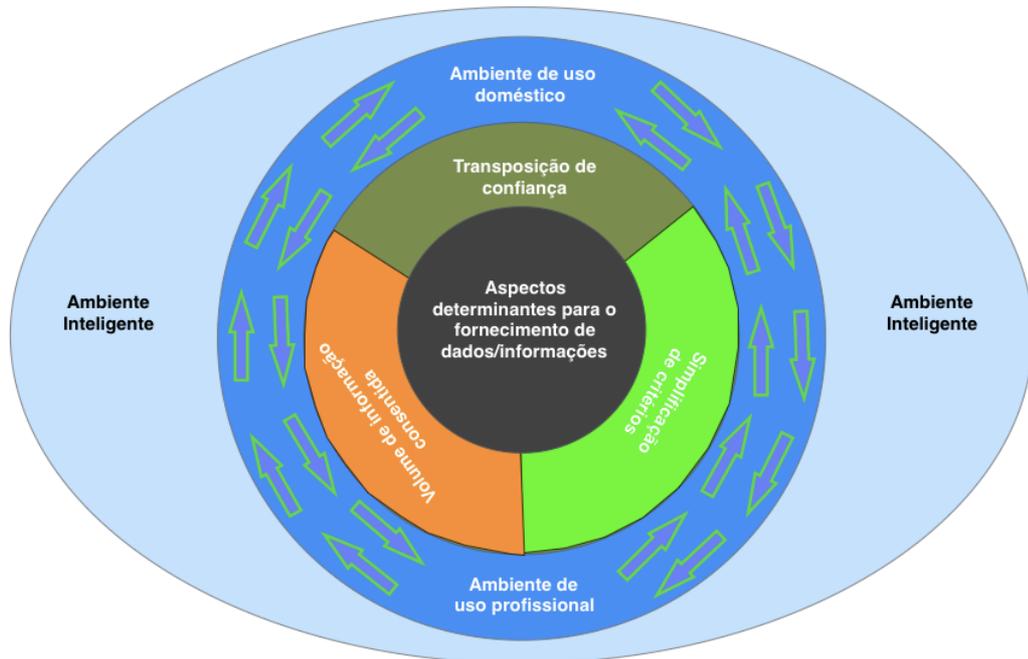
4) A simplificação dos critérios caracteriza-se pelo comportamento do usuário de tender sempre a escolhas menos complexas, simplificando sempre que possível seus critérios de segurança para disponibilizar informação. Ao comportar-se segundo este aspecto o usuário tende a abrir mão de uma análise própria e detalhada, fazendo suas escolhas baseado em informações mínimas e de fácil acesso, porém não verificadas.

Este aspecto desperta preocupação, como destaca Krause (2009) e Chabridon *et al.* (2014), visto que a simplificação pode ocasionar o desconhecimento por parte do usuário de fatores chave relacionados a sua privacidade no ambiente inteligente. Todavia como destaca Weber (2010) as empresas desenvolvedoras das soluções têm obrigação de adequarem-se a realidade dos usuários e de proverem soluções tecnológicas cada vez mais amigáveis e de compreensão facilitada.

Diante de tal afirmação, corrobora-se com Kranz, Roalter e Michahelles (2010) desconsiderando a possibilidade de mudança de comportamento do usuário em curto prazo, observa-se neste aspecto uma questão que determina não apenas o fornecimento de informações para o ambiente inteligente como também uma oportunidade a ser explorada pelas organizações fornecedoras de soluções como meio de atratividade dos usuários, criando resumos de fácil compreensão de políticas de privacidade para a relação entre usuário e ambiente inteligente por meio de seus dispositivos.

Com base nesses aspectos, a figura 6, ilustra o cenário encontrado, apresentando dentro do ambiente inteligente os ambientes de uso estudados de maneira integrada entre si, que influenciam nos fenômenos da transposição de confiança, no volume de informação consentida e na simplificação de critérios. Este conjunto de aspectos convergem para a formação dos aspectos determinantes para o fornecimento de informações pessoais em ambientes inteligentes.

**Figura 6:** Aspectos determinantes para o fornecimento de dados e informações em ambientes inteligentes



Fonte: Dados da Pesquisa (2016).

Baseado nestes principais achados o capítulo a seguir apresenta as conclusões deste trabalho, fazendo um confronto entre os objetivos propostos para a pesquisa e os resultados alcançados a fim de responder à pergunta que norteou a pesquisa, apresentar as limitações desta e propostas para estudos futuros.

*“Toda a teoria só é boa na condição de que,  
utilizando-a, se vá mais além”.*

(André Gide)

## 5 CONCLUSÕES

A relevância do papel desempenhado pelas pessoas nas transformações que as implementações de tecnologias baseadas na IoT podem promover e a necessidade de compreender os fatores que estas pessoas percebem como relevantes para fornecerem dados e informações por meio destas tecnologias, motivou a escolha do problema de pesquisa proposto para este estudo - Quais aspectos determinam a ação dos usuários ao fornecerem informações pessoais em ambientes inteligentes?

Tal questionamento ganha resposta a partir da identificação dos tipos de tecnologias inteligentes utilizadas pelos usuários, da descrição das formas de uso cotidiana das tecnologias inteligentes, da identificação dos tipos de dados e informações fornecidas em ambientes inteligentes e da análise dos aspectos determinantes para o fornecimento desse dados e informações. Os principais resultados encontrados foram sintetizados no quadro 11 e na figura 6, presentes na seção de análise dos dados deste estudo.

Dentre as principais conclusões decorrentes da pesquisa, intuiu-se que o ambiente de uso se configura como um aspecto determinante ao fornecimento de informação ao ambiente inteligente de maior influência entre os outros aspectos encontrados. Relevância já destacada por autores como Atzori, Iera e Giacomo (2010), Eurich, Oertel e Boutellier (2010), Miorandi et al. (2012), Domingo (2012) no tocante a escolha de *hardware* e *software* apropriados por parte de empresas e profissionais, torna-se aqui também evidente sua influência na percepção dos usuários e conseqüentemente nas suas escolhas ao fornecerem informações, compreendendo que o comprometimento da relação entre o usuário e o ambiente de uso possivelmente influenciará sob todos os outros aspectos e nas escolhas do usuário.

Chabrindon *et al.* (2014) apontam que um dos fatores que mais tornam vulneráveis as informações não são as estruturas de *software* e de *hardware*, destacando que o usuário deve ser visto como elemento gerador de vulnerabilidades, os achados da pesquisa permitiram observar tal afirmação em campo destacando que os usuários tendem a dedicar considerável atenção a segurança e a privacidade das informações que possuem, disponibilizando-as com ressalvas e cuidados. Contudo por vezes, transferem a responsabilidade pela segurança das informações para

terceiros, buscando reduzir ao máximo o número de critérios a serem analisados antes de tomar a decisão de disponibilizar seus dados.

No entanto, observou-se a preocupação das empresas com a segurança da informação demonstrada pela existência de profissionais especializados que orientam regras de segurança e auxiliam na análise e na escolha, entre os aspectos analisados, buscando equilíbrio entre os recursos disponíveis. Isto gera resultados positivos também no ambiente doméstico, tendo em vista que mesmo as escolhas, que são realizadas dentro do ambiente profissional com auxílio especializado não sendo levadas para o ambiente doméstico de maneira direta, a comunicação constante dos usuários em ambos os ambientes faz com que um possa influenciar o outro.

Tal fenômeno acontece porquê o comportamento do usuário em relação a sua percepção de privacidade e o que a influência ao disponibilizar suas informações pode ser antagônica em situações distintas, no entanto não se pode ignorar por completo o conhecimento prévio adquirido em outras experiências do usuário (MARX, 2001).

Do ponto de vista da aceitação por parte do usuário, o panorama para implementação de soluções pautadas em tecnologias baseadas na Internet das Coisas no Brasil é positivo. Mesmo com o elevado preço dos dispositivos inteligentes hoje disponíveis no mercado, já é possível encontrá-los com facilidades entre os usuários. Do ponto de vista da segurança da informação e manutenção da privacidade, o cenário é promissor já que engloba usuários que buscam ativamente mais praticidade e também profissionais dedicados a essa realidade. Assim, acredita-se que novas soluções possam emergir desse cenário nos próximos anos.

No que tange ao conceito mais amplo do ambiente inteligente, enquanto ambiente integrado e conectado, observa-se no Brasil que ainda é uma realidade em construção, como encontrado na literatura internacional (ATZORI; IERA; GIACOMO, 2010; EURICH; OERTEL; BOUTELLIER, 2010; MIORANDI et al., 2012; PEOPLES et al., 2013; GUBBI et al., 2013; CHABRINDON et al., 2014; DUTTON, 2014) e está em franco crescimento. No entanto ainda com poucas definições e sem propensões imediatas de atingir seu construto por completo.

Por fim, afirma-se que a Internet das Coisas como objeto de estudo ainda está em estado embrionário em aspectos chaves como a privacidade do usuário, a destinação da informação, a conveniência das soluções para o usuário e autonomia

de escolha do usuário, e por isto, a percepção dos usuários a respeito do que pode ser determinante ou não ainda sofrerá mudanças antes que uma estrutura mais ampla de ambiente inteligente esteja em total funcionamento. Sendo esses usuários um público de maior grau de instrução, os mesmos podem contribuir ativamente para essa implementação, tornando não apenas o investimento em tecnologia, mas também o investimento em educação essencial para a evolução e implementação da Internet das Coisas.

### 5.1 Limitações do Estudo

Inicialmente, foi realizado o levantamento teórico a respeito do tema na literatura nacional, na qual constatou-se ainda ser reduzido os estudos a respeito da Internet das Coisas, no entanto na literatura internacional, foi possível encontrar pesquisas correlatas em maior quantidade e qualidade. Após análise da literatura encontrada, foi possível realizar as escolhas filosóficas e metodológicas da pesquisa buscando interligar os objetivos da pesquisa com a temática a ser estudada.

Na etapa de coleta dos dados, aponta-se como limitações as restrições financeiras, visto que durante a realização da pesquisa, não houveram recursos financeiros disponíveis para o deslocamento que permitisse a aplicação presencial dos questionários com respondentes em outras regiões do país. Para minimizar essa limitação, foram utilizadas duas bases de dados de usuários previamente cadastrados a [survio.com](http://survio.com) e a [surveymonkey.com](http://surveymonkey.com). Ressalta-se também a limitação temporal, já que a necessidade do cumprimento dos prazos do programa de pós-graduação não permitiu um corte temporal mais extenso para a coleta de dados em campo.

Durante a etapa de tratamento dos dados a pesquisa limitou-se aos dados provenientes de usuários residentes no Brasil, que possuíssem um mínimo de dois dispositivos inteligentes e que tivessem idade igual ou superior a 15 anos, considerando inválidos e eliminando respondentes que se enquadrassem fora desses limites.

Em relação aos tipos de dispositivos contemplados pela pesquisa, limitou-se a considerar dispositivos inteligentes, os dispositivos com capacidade de conectividade e interação através de soluções pautadas em tecnologias da Internet das Coisas, seja em ambiente doméstico ou profissional, excluindo outros dispositivos apontados pelos respondentes que não se enquadrassem nesses requisitos.

Destaca-se também, a difícil missão de encontrar e atribuir definições a construtos, aspectos e ideias ainda em seu estágio inicial, onde a literatura existente não converge para um conceito único dos fenômenos existentes e outros ainda estão sendo descobertos exigindo do pesquisador maior perspicácia em relação as escolhas feitas para a construção da pesquisa.

## 5.2 Indicações para Futuras Pesquisas

Quanto as indicações para futuras pesquisas, recomenda-se que sejam realizados estudos voltados para a construção de elementos simplificados destinados para a segurança da informação e para o gerenciamento da privacidade, a fim de melhor explorar o comportamento voltado a simplificação de critérios identificado nos usuários.

Sugere-se a exploração da relação da transposição de confiança, realizando estudos que possam identificar quais dos elementos geradores de confiança nos consumidores em relação marcas e organizações podem ser atribuídos a construção da relação de confiança entre o usuário e o ambiente inteligente. A realização de estudos que possam comparar a realidade brasileira aqui encontrada com a realidade de outros países em patamar semelhante de desenvolvimento econômico e social encontrados na América Latina e a comparação com países desenvolvidos da América do Norte, Europa e Ásia.

Por fim, destaca-se serem necessários mais estudos voltados as mais variadas possibilidades de aplicações da Internet das Coisas, por tratar-se de um conjunto complexo de fatores que envolvem governos, empresas, instituições militares e civis, que sendo utilizado da maneira adequada pode vir a beneficiar toda a sociedade, mas que também podem expor a riscos de segurança em nível pessoal e coletivo, e por isto torna-se necessário uma maior atenção e reflexão por toda a população e por organizações de todos os setores.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, José Augusto Lindgren. A declaração dos direitos humanos na pós-modernidade. **Os direitos humanos e o direito internacional**. Rio de Janeiro: **Renovar**, p. 139-166, 1999.

ASHRAF, Qazi Mamoon; HABAEBI, Mohamed Hadi. Autonomic schemes for threat mitigation in Internet of Things. **Journal of Network and Computer Applications**, v. 49, p. 112-127, 2015.

ASHTON, Kevin. That 'internet of things' thing. **RFID Journal**, v. 22, n. 7, p. 97-114, 2009.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. **Computer networks**, v. 54, n. 15, p. 2787-2805, 2010.

BERNERS-LEE, Tim; O'HARA, Kieron. The read-write Linked Data Web. **Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences**, v. 371, n. 1987, p. 20120513, 2013.

BITTERMANN, Henry J. Adam Smith's empiricism and the law of nature: I. **The Journal of Political Economy**, p. 487-520, 1940.

BOTTERMAN, M. for the European Commission Information Society and Media Directorate General. In: **Networked Enterprise & RFID Unit-D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic**. 2009.

BRODY, Paul; PURESWARAN, Veena. The next digital gold rush: how the internet of things will create liquid, transparent markets. **Strategy & Leadership**, v. 43, n. 1, p. 36-41, 2015.

BRUNI, Adriano Leal. SPSS Guia Prático para Pesquisadores. **São Paulo: Atlas**, p. 280, 2012.

BUCKL, Christian et al. Services to the field: An approach for resource constrained sensor/actor networks. In: **Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on**. IEEE, 2009. p. 476-481.

BURRELL, Gibson; MORGAN, Gareth. **Sociological paradigms and organisational analysis**. London: Heinemann, 1979.

BUSSAB, Wilton O.; MORETTIN, Pedro A. Estatística básica. 5ª. **São Paulo: Editora Saraiva**, 2003.

CASTELLUCCIA, Claude et al. Privacy, accountability and Trust-Challenges and opportunities. **ENISA.[Online]. Available: <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study/atdownload/fullReport>**, 2011.

CHABRIDON, Sophie et al. A survey on addressing privacy together with quality of context for context management in the Internet of Things. **annals of telecommunications-Annales des télécommunications**, v. 69, n. 1-2, p. 47-62, 2014.

CHAOUCHI, Hakima (Ed.). **The internet of things: connecting objects**. John Wiley & Sons, 2013.

CHAUÍ, Marilena. Convite à filosofia. **São Paulo: Ática**, 2002.

CLARK, Andrew. Public Access to the English Coastline: An Analysis of Part 9 of the Marine and Coastal Access Bill. **Liverpool Law Review**, v. 30, n. 2, p. 147-171, 2009.

COMPARATO, FABIO KONDER. **A AFIRMAÇÃO HISTÓRICA DOS DIREITOS HUMANOS**. 2010. Tese de Doutorado. Universidade de Coimbra.

CUSUMANO, M.; GOELDI, ANDREAS; DUTTON,. New businesses and new business models. **W. Dutton, The Oxford handbook of Internet**, p. 239-261, 2013.

DANEZIS, George; GÜRSES, Seda. A critical review of 10 years of privacy technology. **Proceedings of Surveillance Cultures: A Global Surveillance Society**, 2010.

DARIANIAN, Mohsen; MICHAEL, Martin Peter. Smart home mobile RFID-based Internet-of-Things systems and services. In: **Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on**. IEEE, 2008. p. 116-120.

DE SOUZA, Nali de Jesus. Desenvolvimento econômico. **Revista de Economia Política**, v. 14, n. 2, p. 54, 1994.

DOMINGO, Mari Carmen. An overview of the Internet of Things for people with disabilities. **Journal of Network and Computer Applications**, v. 35, n. 2, p. 584-596, 2012.

DOMINGO, Mari Carmen. An overview of the internet of underwater things. **Journal of Network and Computer Applications**, v. 35, n. 6, p. 1879-1890, 2012.

DUTTON, William H. The Internet and social transformation: reconfiguring access. Transforming enterprise: **The economic and social implications of information technology**, p. 375-397, 2005.

EURICH, Markus; OERTEL, Nina; BOUTELLIER, Roman. The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain. **Electronic Commerce Research**, v. 10, n. 3-4, p. 423-440, 2010.

FLOERKEMEIER, Christian; RODUNER, Christof; LAMPE, Matthias. RFID application development with the Accada middleware platform. **Systems Journal, IEEE**, v. 1, n. 2, p. 82-94, 2007.

FREITAS, Henrique et al. O método de pesquisa survey. **Revista de Administração da Universidade de São Paulo**, v. 35, n. 3, 2000.

GAO, Lingling; BAI, Xuesong. A unified perspective on the factors influencing consumer acceptance of internet of things technology. **Asia Pacific Journal of Marketing and Logistics**, v. 26, n. 2, p. 211-231, 2014.

GREER, Steven. **The European Convention on Human Rights: achievements, problems and prospects**. Cambridge University Press, 2006.

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. **Future Generation Computer Systems**, v. 29, n. 7, p. 1645-1660, 2013.

GUERRA, G. A. et al. **Economics of trust: Trust and the information economy**. DSTI/ICCP/IE/REG (2002) 2, OECD, Paris and OII Research Report, 2003.

H. DUTTON, William. Putting things to work: social and policy challenges for the Internet of things. **info**, v. 16, n. 3, p. 1-21, 2014.

KRANZ, Matthias; ROALTER, Luis; MICHAHELLES, Florian. Things that twitter: social networks and the internet of things. In: What can the Internet of Things do for the Citizen (CIoT) Workshop at The Eighth International Conference on Pervasive Computing (Pervasive 2010). 2010. p. 1-10.

KRAUSE, Michael; HOCHSTATTER, Iris. Challenges in modelling and using quality of context (qoc). In: **Mobility aware technologies and applications**. Springer Berlin Heidelberg, 2005. p. 324-333.

KRÜCKEN, Georg. Learning theNew, New Thing': On the role of path dependency in university structures. **Higher Education**, v. 46, n. 3, p. 315-339, 2003.

KRUMM, John. A survey of computational location privacy. **Personal and Ubiquitous Computing**, v. 13, n. 6, p. 391-399, 2009.

LANGHEINRICH, Marc. A survey of RFID privacy approaches. **Personal and Ubiquitous Computing**, v. 13, n. 6, p. 413-421, 2009.

LEWIS, Philip; THORNHILL, Adrian; SAUNDERS, M. **Research methods for business students**. Pearson Education UK, 2007.

LI, Shancang; DA XU, Li; ZHAO, Shanshan. The internet of things: a survey. **Information Systems Frontiers**, v. 17, n. 2, p. 243-259, 2014.

MARX, Gary T. Murky conceptual waters: The public and the private. **Ethics and Information technology**, v. 3, n. 3, p. 157-169, 2001.

MATOS, Alfredo Miguel Melo. Privacy in next generation networks. 2012.

MEIRELLES, Fernando de Souza. 25ª Pesquisa Anual do Uso de TI, 2014.

MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. **Ad Hoc Networks**, v. 10, n. 7, p. 1497-1516, 2012.

PAMPLONA FILHO, Rodolfo. LEI Nº 12.965, DE 23 ABRIL DE 2014. **Direito UNIFACS–Debate Virtual**, n. 167, 2014.

PANG, Zhibo et al. Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. **Enterprise Information Systems**, v. 9, n. 1, p. 86-116, 2015.

PEOPLES, Cathryn et al. Performance evaluation of green data centre management supporting sustainable growth of the internet of things. **Simulation Modelling Practice and Theory**, v. 34, p. 221-242, 2013.

PIOVESAN, Flávia. Direitos humanos. **Curitiba: Juruá**, v. 1, p. 15-37, 2006.

PRESSER, Mirko; GLUHAK, Alexander. The internet of things: Connecting the real world with the digital world. **EURESCOM mess@ ge–The Magazine for Telecom Insiders**, v. 2, 2009.

ROCHA, Luiz Célio Souza; DE ARAÚJO, Geyson Eliakim Ferreira; MARQUES, Robson Oliveira. ABORDAGENS EPISTEMOLÓGICAS NAS PESQUISAS EM ADMINISTRAÇÃO: UMA ANÁLISE NAS DISSERTAÇÕES DE UM PROGRAMA DE PÓS-GRADUAÇÃO NO NORDESTE BRASILEIRO. **HOLOS**, v. 4, p. 126-147, 2012.

ROCHELANDET, Fabrice; TAI, Silvio HT. Do privacy laws affect the location decisions of internet firms? Evidence for privacy havens. **European Journal of Law and Economics**, p. 1-30, 2012.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the internet of things. **Computer**, v. 44, n. 9, p. 51-58, 2011.

SARMA, Sanjay E.; WEIS, Stephen A.; ENGELS, Daniel W. RFID systems and security and privacy implications. In: **Cryptographic Hardware and Embedded Systems-CHES 2002**. Springer Berlin Heidelberg, 2003. p. 454-469.

SAXBY, Steve. The 2014 CLSR-LSPI Lisbon seminar on ‘the digital citizen’—Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15–17 October 2014, Vieira De Almeida & Associados, Lisbon, Portugal. **Computer Law & Security Review**, v. 31, n. 2, p. 163-180, 2015.

SCHRADER, Achim; MALWITZ-SCHÜTTE, Magdalene; SELL, Jürgen. **Introdução à pesquisa social empírica: um guia para o planejamento, a execução ea avaliação de projetos de pesquisa nao-experimentais**. Globo, Ed. da Universidade Federal do Rio Grande do Sul, 1974.

SERVA, Maurício. O surgimento e o desenvolvimento da epistemologia da administração–inferências sobre a contribuição ao aperfeiçoamento da teoria administrativa. **Revista Gestão Organizacional**, v. 6, n. 3, 2014.

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania law review**, p. 477-564, 2006.

SOUZA, Ivone Gomes de Assis. Uma análise das abordagens epistemológicas e metodológicas da pesquisa contábil no programa do mestrado multiinstitucional em ciências contábeis. **Convênio UNB, UFPB, UFPE e UFRN**, 2005.

STEFFEK, Jens; NANZ, Patrizia. Emergent patterns of civil society participation in global and European governance. **Civil society participation in European and global governance: A cure for the democratic deficit**, p. 1-29, 2008.

STEVENTON, Alan; WRIGHT, Steve (Ed.). **Intelligent spaces: The application of pervasive ICT**. Springer Science & Business Media, 2010.

STRATEGY, I. T. U.; UNIT, Policy. ITU Internet Reports 2005: The internet of things. **Geneva: International Telecommunication Union (ITU)**, 2005.

TRIVISIOS, Augusto NS. Introdução a pesquisa em ciências sociais. **A Pesquisa**, 1987.

UNITED NATIONS ORGANIZATION. **Global Reporto f the Online Population**. Internacional Telecommunication Union, 2015.

URNAUER, Suellem Aparecida; MENNA BARRETO, Ricardo de Macedo. SEGURANÇA JURÍDICA NA CIBERCULTURA DE CONSUMO: REFLEXÕES À LUZ DA LEI Nº 12.965/2014 (MARCO CIVIL DA INTERNET). **Revista do Mestrado em Direito da Universidade Católica de Brasília: Escola de Direito**, v. 8, n. 2, p. 263-287, 2015.

VAIDYA, Jaideep. Privacy in the context of digital government. In: **Proceedings of the 13th Annual International Conference on Digital Government Research**. ACM, 2012. p. 302-303.

VALÉRY, N. Welcome to the Thingtnet: Things, Rather than People, are About to Become the Biggest Users of the Internet. **The Economist**, v. 21, 2012.

VAN DEN BOSSCHE, Peter. Ngo Involvement in the Wto: A Comparative Perspective. **Journal of International Economic Law**, v. 11, n. 4, p. 717-749, 2008.

VASSEUR, J. et al. RPL: The IP routing protocol designed for low power and lossy networks. **Internet Protocol for Smart Objects (IPSO) Alliance**, v. 36, 2011.

VASSEUR, Jean-Philippe; DUNKELS, Adam. **Interconnecting smart objects with ip: The next internet**. Morgan Kaufmann, 2010.

WANG, Yang; KOBASA, Alfred. Privacy-enhancing technologies. **Handbook of Research on Social and Organisational Liabilities in Information Security**, p. 203-227, 2008.

WEBER, Rolf H. Internet of Things—New security and privacy challenges. **Computer Law & Security Review**, v. 26, n. 1, p. 23-30, 2010.

WEBER, Rolf H.; WEBER, Romana. **Internet of Things**. New York: Springer, 2010.

WELBOURNE, Evan et al. Building the internet of things using RFID: the RFID ecosystem experience. **Internet Computing, IEEE**, v. 13, n. 3, p. 48-55, 2009.

ZANELLA, Liane Carly Hermes. Metodologia de estudo e de pesquisa em administração. **Florianópolis: Departamento de Ciências da Administração/UFSC**, 2009.

ZHENG-QIANG, Liang; WEI-SONG, Shi. Enforcing cooperative resource sharing in untrusted Peer-to-Peer environments. **Journal of Mobile Networks and Applications-Springer**, v. 10, n. 6, p. 771-783, 2005.

ZORZI, Michele et al. From today's intranet of things to a future internet of things: a wireless-and mobility-related view. **Wireless Communications, IEEE**, v. 17, n. 6, p. 44-51, 2010.

## APÊNDICE A: INSTRUMENTO DE COLETA DE DADOS

AS PERGUNTAS DE 1 A 4 DIZEM RESPEITO AO SEU PERFIL, ASSINALE APENAS UM ITEM EM CADA PERGUNTA E SENDO ESTE O QUE MAIS SE APROXIMAR DA SUA REALIDADE.

1 - Assinale o em relação ao gênero:

- Masculino
- Feminino

2 - Assinale a faixa etária que melhor representa você atualmente:

- de 15 - 20 anos
- de 21 - 25 anos
- de 26 - 30 anos
- de 31 - 35 anos
- de 36 - 40 anos
- acima de 40 anos

3 - Assinale em qual região do Brasil você vive:

- Norte
- Nordeste
- Centro-Oeste
- Sul
- Sudeste

4 - Assinale o seu grau de escolaridade:

- Ensino fundamental incompleto
- Ensino fundamental completo
- Ensino médio incompleto
- Ensino médio completo
- Ensino técnico
- Ensino superior incompleto
- Ensino superior completo
- Pós-graduação (*Lato Sensu e Stricto Sensu*)
- Outros \_\_\_\_\_

AS PERGUNTAS DE 5 A 7 DIZEM RESPEITO AOS DISPOSITIVOS QUE VOCÊ POSSUI E UTILIZA, ASSINALE QUANTOS ITENS CONSIDERAR NECESSÁRIO E UTILIZE O CAMPO OUTROS CASO NECESSITE INDICAR ALGO NÃO CONTEMPLADO NAS ALTERNATIVAS DISPONÍVEIS.

5 - Assinale quais dispositivos inteligentes você possui:

- Relógio Inteligente (*Smart Watch*)
- TV Inteligente (*Smart TV*)
- Telefone Inteligente (*SmartPhone*)
- Aparelho de som Inteligente (*Smart Stereo*)
- Pulseira Inteligente (*Smart Bracelet*)
- GPS Inteligente (*GPS Smart*)
- Agenda Inteligente (*Smart Calendar*)
- Óculos Inteligente (*Smart Glasses*)
- Itens de vestuário esportivo como camisetas, viseiras, bones, tenis, bermudas, etc
- Outros \_\_\_\_\_

6 - Assinale quais dispositivos inteligentes você utiliza diariamente:

- Relógio Inteligente (*Smart Watch*)
- TV Inteligente (*Smart TV*)
- Telefone Inteligente (*SmartPhone*)
- Aparelho de som Inteligente (*Smart Stereo*)
- Pulseira Inteligente (*Smart Bracelet*)
- GPS Inteligente (*GPS Smart*)
- Agenda Inteligente (*Smart Calendar*)
- Óculos Inteligente (*Smart Glasses*)
- Itens de vestuário esportivo como camisetas, viseiras, bones, tenis, bermudas, etc
- Outros \_\_\_\_\_

7 - Assinale quais dispositivos inteligentes você possui que estão em desuso:

- Relógio Inteligente (*Smart Watch*)
- TV Inteligente (*Smart TV*)
- Telefone Inteligente (*SmartPhone*)
- Aparelho de som Inteligente (*Smart Stereo*)
- Pulseira Inteligente (*Smart Bracelet*)
- GPS Inteligente (*GPS Smart*)
- Agenda Inteligente (*Smart Calendar*)
- Óculos Inteligente (*Smart Glasses*)
- Itens de vestuário esportivo como camisetas, viseiras, bones, tenis, bermudas, etc
- Outros \_\_\_\_\_

AS PERGUNTAS DE 8 A 13 DIZEM RESPEITO A FORMA DE USO DOS DISPOSITIVOS QUE VOCÊ POSSUI E UTILIZA, ASSINALE QUANTOS ITENS CONSIDERAR NECESSÁRIO E UTILIZE O CAMPO OUTROS CASO NECESSITE INDICAR ALGO NÃO CONTEMPLADO NAS ALTERNATIVAS DISPONÍVEIS.

8 - Assinale os ambientes que você utiliza seus dispositivos inteligentes:

Ambientes públicos

- Praças
- Parques
- Praias
- Trilhas
- Academia
- Museus
- Cinemas
- Shoppings
- Outros \_\_\_\_\_

Ambientes privados de uso comum

- Casa
- Condômino
- Apartamento
- Hotéis
- Outros \_\_\_\_\_

Ambientes profissionais

- Trabalho
- Escritório em casa (Home Office)
- Empresa
- Escola
- Faculdade e/ou universidade
- Em viagens a trabalho
- Outros \_\_\_\_\_

9 - Assinale os ambientes que você **evita** utilizar seus dispositivos inteligentes?

Ambientes públicos

- Praças
- Parques
- Praias
- Academia
- Trilhas
- Museus
- Cinemas
- Shoppings
- Outros \_\_\_\_\_

## Ambientes privados de uso comum

- Casa
- Condômino
- Apartamento
- Hotéis
- Outros \_\_\_\_\_

## Ambientes profissionais

- Trabalho
- Escritório em casa (Home Office)
- Empresa
- Escola
- Faculdade e/ou universidade
- Em viagens a trabalho
- Outros \_\_\_\_\_

## 10 - Assinale para quais finalidades você utiliza seus dispositivos:

- Acesso a internet
- Consultar a previsão do tempo
- Consultar o trânsito
- Acesso a redes sociais
- Mensagens instantâneas
- Acesso a notícias
- Entretenimento (músicas e filmes)
- Acesso a serviços públicos (agendamento de horários, requerimentos on-line, atendimentos virtual, etc)
- Consulta a mapas e endereços (Geolocalização)
- Busca por empresas (lojas comerciais, prestadores de serviço, restaurantes, postos de combustíveis, etc)
- Monitoramento de segurança (Alarmes e trancas, sistema interno de TV, localização em tempo real, etc)
- Acompanhamento físico e de saúde (pressão arterial, batimentos cardíacos, consumo calórico, horas de sono, etc)
- Outros \_\_\_\_\_

11 - Assinale para quais finalidades você **evita** utilizar seus dispositivos:

- Acesso a internet
- Consultar a previsão do tempo
- Consultar o trânsito
- Acesso a redes sociais
- Mensagens instantâneas
- Acesso a notícias
- Entretenimento (músicas e filmes)
- Acesso a serviços públicos (agendamento de horários, requerimentos on-line, atendimentos virtual, etc)
- Consulta a mapas e endereços (Geolocalização)
- Busca por empresas (lojas comerciais, prestadores de serviço, restaurantes, postos de combustíveis, etc)
- Monitoramento de segurança (Alarmes e trancas, sistema interno de TV, localização em tempo real, etc)
- Acompanhamento físico e de saúde (pressão arterial, batimentos cardíacos, consumo calórico, horas de sono, etc)
- Outros \_\_\_\_\_

12 - Assinale as **três** principais finalidades para qual você utiliza seus dispositivos:

- Acesso a internet
- Consultar a previsão do tempo
- Consultar o trânsito
- Acesso a redes sociais
- Mensagens instantâneas
- Acesso a notícias
- Entretenimento (músicas e filmes)
- Acesso a serviços públicos (agendamento de horários, requerimentos on-line, atendimentos virtual, etc)
- Consulta a mapas e endereços (Geolocalização)
- Busca por empresas (lojas comerciais, prestadores de serviço, restaurantes, postos de combustíveis, etc)
- Monitoramento de segurança (Alarmes e trancas, sistema interno de TV, localização em tempo real, etc)
- Acompanhamento físico e de saúde (pressão arterial, batimentos cardíacos, consumo calórico, horas de sono, etc)
- Outros \_\_\_\_\_

AS PERGUNTAS DE 13 A 18 DIZEM RESPEITO AOS TIPOS DE DADOS E INFORMAÇÕES QUE VOCÊ FORNECE POR MEIO DE SEUS DISPOSITIVOS, ASSINALE QUANTOS ITENS CONSIDERAR NECESSÁRIO E UTILIZE O CAMPO OUTROS CASO NECESSITE INDICAR ALGO NÃO CONTEMPLADO NAS ALTERNATIVAS DISPONÍVEIS.

13 - Assinale quais dados pessoais você disponibiliza em seus dispositivos:

- Nome
- Nome completo
- Endereço de casa
- Endereço do trabalho
- Telefone residencial
- Telefone celular
- Telefone do trabalho
- E-mail pessoal
- E-mail profissional
- Idade e/ou data de nascimento
- Documentos oficiais (carteira de identidade, CPF, registro profissional, etc)
- Dados bancários
- Cidade de origem
- Outros \_\_\_\_\_

14 - Assinale quais dados pessoais você **evita** disponibilizar em seus dispositivos:

- Nome
- Nome completo
- Endereço de casa
- Endereço do trabalho
- Telefone residencial
- Telefone celular
- Telefone do trabalho
- E-mail pessoal
- E-mail profissional
- Idade e/ou data de nascimento
- Documentos oficiais (carteira de identidade, CPF, registro profissional, etc)
- Dados bancários
- Cidade de origem
- Outros \_\_\_\_\_

15 - Assinale quais informações você fornece com frequência em seus dispositivos em **uso domésticos**:

- Informações de membros familiares
- Agenda de contatos e compromissos
- Localização atual e destino

- Condições de saúde
- Preferencias de alimentação
- O que você está fazendo em tempo real
- Com quem você está e/ou com quem estará
- Outros \_\_\_\_\_

16 - Assinale quais informações você fornece com frequência em seus dispositivos em **uso profissional**:

- Informações de membros familiares
- Agenda de contatos e compromissos
- Localização atual e destino
- Condições de saúde
- Preferencias de alimentação
- O que você está fazendo em tempo real
- Com quem você está e/ou com quem estará
- Outros \_\_\_\_\_

17 - Assinale as condições que determinam o fornecimento de informações a seus dispositivos em ambientes domésticos:

- Confiança na plataforma e/ou na empresa responsável pelo dispositivo
- Controle de quem acessa a informação fornecida
- Possibilidade de verificação das informações sempre que desejar
- Capacidade de alterar ou remover a informação fornecida
- Anonimato da informação fornecida
- Escolha de quais informações fornecer
- Facilidade de uso do dispositivo
- Saber a que uso se destina a informação coletada
- Política de privacidade clara e objetiva
- Ser notificado quanto ao uso de informações por terceiros
- Outros \_\_\_\_\_

18 - Assinale as condições que determinam o fornecimento de informações a seus dispositivos em ambientes profissionais?

- Confiança na plataforma e/ou na empresa responsável pelo dispositivo
- Controle de quem acessa a informação fornecida
- Possibilidade de verificação das informações sempre que desejar
- Capacidade de alterar ou remover a informação fornecida
- Anonimato da informação fornecida
- Escolha de quais informações fornecer
- Facilidade de uso do dispositivo
- Saber a que uso se destina a informação coletada
- Política de privacidade clara e objetiva
- Ser notificado quanto ao uso de informações por terceiros
- Outros \_\_\_\_\_