EJABM European Journal of Applied Business and Management

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Research Paper

O Paradoxo da Privacidade e a Utilização de Tecnologias da Internet Das Coisas

The Privacy Paradox and the Use of IoT Technologies

Submitted in 3, September 2020
Accepted in 16, December 2020
Evaluated by a double blind review system

CARLOS CESAR SANTOS[1*]
JEFFERSON DAVID ARAUJO SALES[2]

Resumo

Objetivo: O presente estudo objetivou investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Coisas ao fornecerem informações pessoais em ambientes inteligentes.

Metodologia: Caracterizou-se como quantitativa, do tipo exploratória e descritiva, implementada por meio da pesquisa de campo, utilizando-se de um questionário autoaplicável.

Originalidade: O presente estudo apresenta os aspectos que determinam a disponibilização de dados pessoais em ambientes inteligentes por parte de usuários brasileiros, explorando o comportamento de uso de uma tecnologia em expansão, no contexto de um país de economia emergente.

Resultados: 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.

Implicações práticas: Numa perspectiva interdisciplinar, este estudo apresenta contributos para o campo da gestão ao fornecer sustentação teórico-empírica para a criação de estratégias de captação de informação e melhoria na experiência dos clientes.

Limitações da investigação: A principal limitação foi a amostra utilizada, recomenda-se que novos estudos sejam realizados para investigar em outros países com contextos culturais e econômicos diferentes, a fim de observar se os aspectos encontrados na amostra brasileira se repetem.

Palavras-chaves: Internet das Coisas; Privacidade; Ambiente Inteligente; Paradoxo da Privacidade.

[1]* Autor correspondente. Faculdade de Administração – FAD, Universidade Federal do Sul e Sudeste do Pará – Unifesspa, Brasil. E-mail: cordcesar@hotmail.com.
[2] Departamento de Administração – DAD, Universidade Federal de Sergipe – UFS, Brasil. E-mail: profsales@hotmail.com.

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Abstract

Objective: The present study aimed to investigate the aspects that determine the action of users of Internet of Things technologies when providing personal information on intelligent environments.

Methodology: It was characterized as quantitative, exploratory and descriptive, implemented through field research, using a self-administered questionnaire.

Originality: This study presents the aspects that determine the availability of personal data in intelligent environments by Brazilian users, exploring the behavior of using an expanding technology, in the context of an emerging economy country.

Results: The environment of use is configured as a determining aspect when providing information to the intelligent environment of greatest influence among the other aspects found. It was noticed that users tend to pay attention to the security and privacy of the information they have, making it available with reservations and care. However, sometimes they transfer the responsibility for the security of the information to third parties, seeking to reduce as much as possible the number of criteria to be allowed before making the decision to make their data available.

Practical implications: In an interdisciplinary perspective, this study presents contributions to the management field by providing theoretical-empirical support for the creation of coordinated information capture and improvement in the customer experience.

Research limitations: The main limitation was the sample used, it is recommended that further studies be carried out to investigate in other countries with different cultural and economic contexts, an end of observation if the aspects found in the Brazilian sample are repeated.

Keywords: Internet of Things; Privacy; Intelligent Environment; Privacy Paradox.

1. Introdução

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; Hassan et al., 2020). A Internet das Coisas - 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 (Gerami & Sarihi, 2020; Peoples et al., 2013).

A 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, sensores, atuadores, *gadget* 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 et al., 2010; Turchet et al., 2020).

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. Intendida como uma

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

questão crucial que pode limitar a implantação da visão IoT seja para usuários privados ou para organizações (Chabridon et al., 2014; Sun & Badi, 2020).

As preocupações relacionadas ao controle da privacidade na IoT já é um aspecto destacado por autores como (Atzori et al., 2010; Chabridon et al., 2014; Chatterjee, 2020; Dutton & William, 2014; Maati & Saidouni, 2020; Prakash & Saini, 2020) 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.

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. Preocupação justificada visto que o Brasil apresenta um panorama favorável a implantação deste tipo de tecnologia, pois a população brasileira já possui aproximadamente 424 milhões de dispositivos conectáveis a internet, isto é, 2 dispositivos para cada 1 habitantes (Meirelles, 2020).

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, objetivando investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Coisas ao fornecerem informações pessoais em ambientes inteligentes.

Este artigo está organizado da seguinte forma. Após esta introdução, apresenta-se na seção 2 a evolução histórica dos padrões de TIC e o surgimento da IoT. Na seção 3 são abordados posicionamentos teóricos a respeito do paradoxo da privacidade e IoT. Na seção 4 são descritos os procedimentos metodológicos e na seção 5 é apresentada a análise dos dados da pequis. Na última seção é destina a discorrer as considerações finais da pesquisa.

2. IoT a 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* (Baiyere et al., 2020; Dutton & William, 2014).

A *Internet of Things* ou Internet das Coisas, como é chamada em português, ganhou uso pela primeira vez em 1999 por Asthon (2010), um dos autores pioneiros nesse tipo de tecnologia, cuja as pesquisas ajudaram a desenvolver o conceito atual desse posicionamento tecnológico. A IoT visa estender a capacidade de conectividade constante, de compartilhamento de dados e do controle a distância para o mundo físico (Peoples et al., 2013). Para alcançar tais pretensões

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

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 (Dutton & William, 2014; Palomino et al., 2020; Santos & Sales, 2018).

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 (Dutton & William, 2014; Saxby, 2015; Vasseur et al., 2011; Zorzi et al., 2010).

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 et al., 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 (Paul, 2015).

O contexto construído até aqui, assume-se que ao unir os termos e apresentá-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 (Ju et al., 2020; Li et al., 2015).

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 et al. (2010) defendem que se deve considerar a Internet das Coisas por meio da convergência dessas três visões. 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* e equipamentos de tecnologia *Near Field Communication* - NFC, tornando estes, componentes chave para a plena 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 et al. (2011) 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 (Vasseur et al., 2011; Zhu et al., 2020). 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 et al., 2010).

Diante de distintas visões de um todo que constitui a Internet das Coisas, Li et al. (2015) 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 pessoas (Valéry, 2012). Logo, como salienta Dutton 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 (Dutton & William, 2014).

O conceito de Internet das Coisas, com sua visão de objetos conectados à internet com variadas capacidades, criam 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, tal conjuntura é definida como ambiente inteligente (Steventon & Wriht, 2010). Os ambientes inteligentes podem impulsionar o papel das TIC's como inovação em uma variedade de mercados de aplicação existentes e que ainda serão criados.

Com destaque aos seis mercados potenciais que podem desempenhar um papel de liderança na adoção de tecnologias da Internet das Coisas já identificados, 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 (Miorandi et al., 2012). E como destaca o autor 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).

3. Paradoxo da privacidade e a IoT

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.,

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

2012; Santos et al., 2015). 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).

A privacidade é agora geralmente percebida pelos usuários como uma expectativa de permanecer num estado de proteção sem ter que o perseguir ativamente (Chabridon et al., 2014). 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 1.

Quadro 1: Linhas de fronteiras pessoais

Linha de fronteira	Descrição
A fronteira natural	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.
A fronteira social	Envolve expectativas que as pessoas com certos papeis sociais como médicos, membros do clero, advogados e outros não irão divulgar informações confidenciais a eles fornecidas pelas pessoas envolvidas.
A fronteira espacial ou temporal	Separa a informação dos vários períodos ou aspectos da vida da pessoa.
A fronteira dos efeitos transitórios	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: Elaboração dos autores com base em Marx (2001)

Solove (2006, 2008) 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 estrapolamento 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 pessoalidade e através da interferência decisória (Solove, 2006, 2008).

Como foi assinalado por Krause & Hochstatter (2005), embora esta taxonomia pretenda ser utilizada para proteção legal, poderá também ser útil para as tecnologias (Hutchison & Mitchell, 1973). 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).

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Baseados nos estudos de Danezis e Gurses (Danezis & Gürses, 2010) foram categorizados 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 (Chabridon et al., 2014).

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 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. Diante dessa perspectiva a privacidade deixou de ser apenas um direito e passou a ser compreendida também como uma capacidade, a capacidade de controlar as como e quais informações sobre si mesmo serão compartilhadas, para quais fins e por quanto tempo (Thomaz et al., 2020).

Neste atual contexto observou-se que mesmo os indivíduos possuindo controle sobre suas informações e declarando o interesse em manter sua privacidade, suas ações nas quais o indivíduos voluntariamente entregam dados e informações pessoais para empresas em troca de pequenos benefícios incompatíveis com o valor do dado que estão disponibilizando evidencia o comportamento paradoxal que norteia essa discussão, definido na literatura como paradoxo da privacidade (Martin, 2020).

O paradoxo da privacidade consiste na contradição entre as preferências de privacidade declaradas pelas pessoas que julgam importante e declaram ter preocupações com sua privacidade e paradoxalmente o seu comportamento real no ambiente on-line divulgam sua informações pessoais e se envolvem em atividades potencialmente prejudiciais para sua privacidade (Martin, 2020). A literatura apresenta três níveis do paradoxo da privacidade, sendo eles o paradoxo forte, o paradoxo fraco e o paradoxo inexistente, esses níveis do paradoxo são conduzidos por abordagens diferentes do conceito de privacidade e da maneira como tal pode ser explorado (Kokolakis, 2017; Martin, 2020).

O paradoxo forte da privacidade caracteriza-se pela interpretação de que a privacidade não existe no mundo on-line, a partir do momento que a pessoa decide estar on-line ela está conscientemente abrindo mão de sua privacidade em detrimento do acesso a rede, de seus produtos e serviços (Barth & de Jong, 2017; Chabridon et al., 2014).

O Paradoxo fraco da privacidade caracteriza-se pela interpretação de que a privacidade é um ativo que pode ser negociado, as pessoas são detentoras de seus dados pessoais e podem decidir negocia-los atribuindo um valor a eles, cabendo as empresas interessadas nesses dados oferecer seus produtos e serviços para que seus clientes percebam uma troca de valor aceitável que justifique abrir mão de sua privacidade individual (Bies & Culnan, 2003; Thomaz et al., 2020).

A ideia do paradoxo inexistente caracteriza-se pela interpretação de que a privacidade é um valor central, fundamental a cada individuo e por isso não pode ser negociada e deve ser preservada independente das declarações ou ações do individuo, sejam essas ações e declarações conscientes ou não, depositando nas organizações a responsabilidade moral e o compromisso ético de preservar a privacidade dos indivíduos (Donaldson & Walsh, 2015; dos Direitos Humanos, 2016).

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Diante dos posicionamentos estabelecidos pelos três níveis do paradoxo da privacidade, privacidade das informações pode, a longo prazo, não ser necessariamente indissolúvel, portanto, estaria nas mãos das empresas a responsabilidade de posicionar suas soluções de IoT de maneira a melhor entregar valor para os seus clientes garantindo uma relação de confiança (Axelson & Bjurström, 2019; Martin, 2020).

4. Procedimentos Metodológicos

A presente pesquisa configura-se como uma pesquisa quantitativa buscando 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.

A natureza do objetivo 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.

O universo de abrangência dessa proposta de pesquisa é formado pelas pessoas que utilizam objetos de tecnologia inteligentes de qualquer natureza como *SmartWatch, SmartTV, SmartPhone, SmartSpeaker, SmartBand, GPS, SmartGlasses,* 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 público alvo foram os usuários de objetos inteligentes conectados a internet cadastrados nos bancos de dados da survio.com e da surveymonkey.com em território brasileiro.

A população brasileira já possui aproximadamente 424 milhões de dispositivos conectáveis a internet, isto é, 2 dispositivos para cada 1 habitantes (Meirelles, 2020), sendo a população brasileira alvo desta pesquisa, enquadra-se esta 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.

Define-se a amostra como por conveniência, por ser adotados respondentes que estão disponíveis em dois bancos de dados já estabelecidos, tal escolha se dá 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 caracteriza 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. Para esta pesquisa, o questionário foi adotado como ferramenta de coleta de dados que contém perguntas de natureza descritiva, comportamental e perguntas preferenciais, podendo serem respondidas de forma objetiva.

5. Análise Dos Dados

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

5.1. Perfil dos respondentes

O rol de sujeitos pesquisados caracteriza-se como uma amostra composta por 228 respondentes, numa distribuição de 41,92% de entrevistados do gênero feminino e 57,64% de entrevistados do gênero masculino. Estes dados iniciais se coadunam com o que apresenta Chabridon et al. (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 (Chabridon et al., 2014). Embora ainda seja observada a predominância do gênero masculino entre os profissionais da área de tecnologia dentro e fora do país (Chatterjee, 2020; Meirelles, 2020; Weber, 2010) o atual equilíbrio no acesso e uso das tecnologias tem potencial para despertar maior interesse nas mulheres em adentrar nesse mercado.

Em relação a faixa etária dos respondentes, observou-se parcial equilíbrio entre a amostra. 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.

Ao estratificar a amostra pelas regiões do país observou-se uma distribuição percentual de 19,65% (centro-oeste), 24,89% (sudeste), 18,34% (sul), 22,27% (nordeste) e 14,41% (norte). 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. 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, 2020).

No que tange ao grau de escolaridade dos respondentes, observou-se que o uso desse tipo de tecnologia no país é democrático, visto que não foi identificado um grau de escolaridade que possa ser destacado como predominante na pesquisa. 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, observando que usuários com maior grau de instrução tendem a facilitar a implantação de inovações por conseguirem utilizar diversos tipos dispositivos sem prejuízos a experiência de uso (Santos, 2015; Vasseur et al., 2011).

Quadro 2: Perfil dos usuários respondentes da pesquisa

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

Fonte: Elaboração dos autores

Partindo dessa característica pode-se traçar um perfil dos usuários, como exposto no quatro 2, os usurários 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

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

mediano. Neste sentido admite-se que as escolhas e comportamentos encontrados neste estudo tem maior predominância para este perfil de usuário.

5.2. Tipos de tecnologias inteligentes

Buscando verificar informações pertinentes quanto a posse e a utilização dos dispositivos os dados da pesquisa apontaram que os dispositivos de tecnologia inteligente mais populares possuídos pelos respondentes da pesquisa, são os *smartphones* e as *smart* TVs com 96,05% e 86,84% dos respondentes declarando possuir um desses dispositivos, respetivamente. O que chama atenção entre os dispositivos inteligentes 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 por Li et al. (2015) é o dispositivo mais utilizado pelos respondentes o que corrobora também com outros autores que mencionam que este artefato se torna um dispositivo indispensável na implementação de interação digitais e de soluções inteligentes (Chabridon et al., 2014; Gama & Santos, 2019). Tal como apontado por Atzori et al. (2010) que relacionam a evolução do uso de aparelhos celulares com a evolução das tecnologias IoT baseada na necessidade de comunicação integrada e continua.

O que se evidencia 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 os dispositivos em desuso, em que 15,79% dos respondentes declaram possuir uma *smart* TV, mas mantém o dispositivo em desuso. Entretanto, a presença da *smart* TV nas residências, mesmo que fora de seu uso diário, configura-se como uma oportunidade, visto que, para alguns autores 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 (Miorandi et al., 2012; Paul, 2015).

5.3. Ambiente de uso dos dispositivos e principais finalidades

Em relação ao ambiente de uso dos dispositivos, observou-se que se torna 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 evidenciadas por Meirelles (2020) 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. Situação que é reforçada em comparação com o ambientes de uso evitados, em que 71,05% dos respondentes afirmaram evitar utilizar seus dispositivos em praças e 63,16% em praias. 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, 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 et al. (2010) já destacaram esta realidade em seu estudo realizado em outros cenários.

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Dentro dessa realidade, ao questionar para quais finalidades os usuários evitavam utilizar seus dispositivos inteligentes, foi possível confirmar, 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 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 (Zorzi et al., 2010).

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. 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*. Contudo destaca-se que no mercado brasileiro, existe um cenário promissor para empresas em outros setores, visto que, 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 (Cusumano & Goeldi, 2013; Paul, 2015).

5.4. Dados e informações disponibilizados por meio dos 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, em que apenas 21,05% dos respondentes declaram disponibilizar seus dados bancários por meio de dispositivos inteligentes. 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, 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 & 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 et al., (2015) ao demonstrar a preocupação dos usuários para com dados de teor financeiro e documentos importantes, trazendo a toma a preocupação dos usuários com a privacidade dentro dos ambientes inteligente. Assim como outros estudos ao tratarem de aplicações de negócios, já destacam que devido a sensação de insegurança e falta de privacidade presente no ambiente inteligente, empresas e usuários mantém soluções inteligentes como soluções secundárias na empresa, resistindo ao uso primário (Ashraf & Habaebi, 2015; Atzori et al., 2010; Miorandi et al., 2012).

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. 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 pesquisadores 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 (Cusumano & Goeldi, 2013; Paul, 2015).

5.5. Aspectos determinantes para o fornecimento de dados e informações

No tocante as condições percebidas pelos usuários como determinantes ao fornecimento de suas informações pessoais. Identificou-se em âmbito doméstico que 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. Este achado corrobora com as afirmações de (Welbourne et al., 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, este fator teve 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 Matthias, Roalter & Michahelles (2010) ao considerarem pouco provável uma mudança no comportamento do usuário apenas pela conscientização do

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

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; Paul, 2015).

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 influência sobre as demais. No entanto, juntas, 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.

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, 2008) 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. 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 1.

Figura 1: Volume de informação consentida

Fonte: Elaboração dos autores

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Em contrapartida, a condição de confiança na plataforma e/ou empresa, 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 significante a escolha das informações de natureza individuais, no entanto as informações de naturezas sociais, não são igualmente influenciadas por esta condição.

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, 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.

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 influência diretamente nos demais fatores. Partindo das linhas de fronteiras pessoais definidas por Marx (2001) tal comportamento pode ser enquadrado na fronteira social, observando 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.

Delegar decisões que dizem respeito a manutenção da privacidade a terceiros podem acarretar em risco à própria essência da privacidade (Chabridon et al., 2014). Neste sentido, credita-se esta preocupação ao fenômeno aqui encontrado, 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.

Para melhor visualizar os achados predominantes atribuídos a esses dados abordados até aqui, o quadro 3 apresenta em resumo as características analisadas, destacando as predominâncias identificadas nos dados coletados em campo.

Quadro 3: Resultados predominantes encontrados em campo

Característica Analisada	Resultado predominante
Dispositivos inteligentes mais populares	S*martphones* 96,05% e as *smart* TVs 86,84%
Dispositivo mais utilizado diariamente	*Smartphones 93,47%*
Dispositivo mais mantido em desuso	Pulseira inteligente 35,53%
Ambiente de uso mais utilizados	Locais de uso comum e fechado: Academia, casa, shopping e faculdade

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Característica Analisada	Resultado predominante
Ambientes de uso mais evitados	Locais abertos: Praças e parques
Finalidade de uso dos dispositivos	Acesso a internet, Mensagens instantâneas e entretenimento
Finalidade de uso mais evitada	Acesso a serviços públicos
Dados e informações disponibilizadas em ambos os ambientes	Agenda de contatos e compromissos, localização atual e destino, condições de saúde e preferência de alimentação
Dados e informações disponibilizadas em uso doméstico	Informações de membros familiares
Dados e informações disponibilizadas em uso professional	Com quem o usuário está e com quem ele estará
Dados e informações que se evita disponibilizar	Dados bancários e documentos oficiais
Aspectos determinantes em ambiente doméstico	Facilidade de uso do dispositivo; confiança na plataforma e/ou na empresa responsável
Aspectos determinantes em ambiente professional	Orientação de profissionais especializados proporcionam equilíbrio entre os aspectos analisados

Fonte: Elaboração dos autores

Com o objetivo de esquematizar os principais achados em campo, a figura 2 destaca os aspectos determinantes para o fornecimento de informações pessoais em ambientes inteligentes, podendo estes serem interpretados dentro do contexto amplo do ambiente inteligente.

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 & Goeldi (2013), assim como de Paul (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;

A transposição de confiança é observada quando o usuário transpõe 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 consequentemente suas informações

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

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, uma vez identificado um padrão emergente de apoio a implementação da IoT, seja explorado como parte integrante do todo (Cusumano & Goeldi, 2013; Paul, 2015);

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;

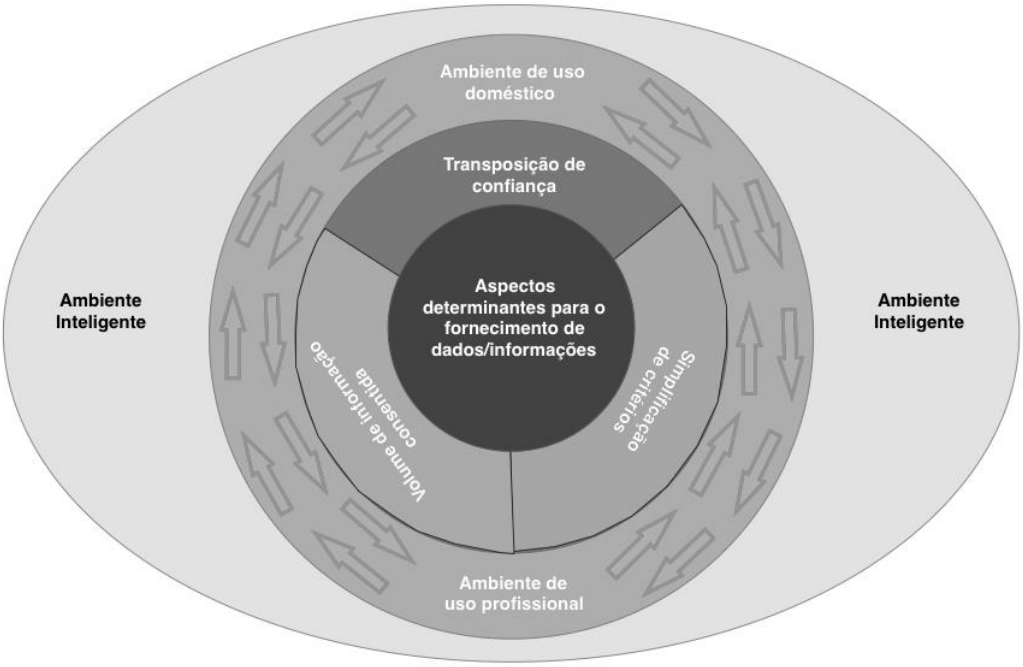
A simplificação dos critérios caracteriza-se pelo comportamento do usuário de tender sempre a escolhas menos complexas, simplificando sempre que possível seus critérios de segurança para disponibilizar informação. Ao comportar-se segundo este aspecto o usuário tende a abrir mão de uma análise própria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

Este aspecto desperta preocupação, visto que a simplificação pode ocasionar o desconhecimento por parte do usuário de fatores chaves relacionados a sua privacidade no ambiente inteligente (Chabridon et al., 2014). Todavia como 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 (Weber, 2010).

Diante de tal afirmação, corrobora-se com Matthias et al. (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.

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

Figura 2: Aspectos determinantes para o fornecimento de dados e informações em ambientes inteligentes



Fonte: Elaboração dos autores

Com base nesses aspectos, a figura 2, 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.

6. Considerações finais

O presente estudo objetivou investigar os aspectos que determinam a ação dos usuários de tecnologias da Internet das Coisas ao fornecerem informações pessoais em ambientes inteligentes. Caracterizou-se como quantitativa, do tipo exploratória e descritiva, implementada por meio da pesquisa de campo, utilizando-se de um questionário autoaplicável.

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 (Atzori et al., 2010; Domingo, 2012; Eurich et al., 2010; Miorandi et al., 2012) no tocante a escolha de *hardware e software* apropriados por parte de empresas e profissionais, torna-se aqui também evidente sua influencia na percepção dos usuários e consequentemente 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.

Um dos fatores que mais tornam vulneráveis as informações não são as estruturas de *software*

European Journal of Applied Business Management, 6(4), 2020, pp. 36-57. ISSN 2183-5594

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 (Chabridon et al., 2014). 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, pois mesmo as escolhas que são realizadas dentro do ambiente profissional com auxilio 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 et al., 2010; Chabridon et al., 2014; Dutton & William, 2014; Eurich et al., 2010; Gubbi et al., 2013; Miorandi et al., 2012; Peoples et al., 2013) 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.

Como principal limitação da pesquisa aponta-se a amostra utilizada que se limitou a usuários residentes no Brasil, por isto recomenda-se como pesquisas futuras a realização de estudos que possam comparar a realidade brasileira 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. Sugere-se também a realização de 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.

Agradecimentos

Esta pesquisa foi desenvolvida com apoio da fundação brasileira Capes – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Referências

Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, *49*, 112–127. https://doi.org/10.1016/j.jnca.2014.11.011

Asthon, K. (2010). That ' Internet of Things ' Thing. *RFID Journal*, 4986. https://doi.org/10.1038/nature03475

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Axelson, M., & Bjurström, E. (2019). The Role of Timing in the Business Model Evolution of Spinoffs: The Case of C3 Technologies. *Research Technology Management*, *62*(4), 19–26. https://doi.org/10.1080/08956308.2019.1613116

Baiyere, A., Topi, H., & Venkatesh, V. (2020). *Internet of Things (IoT)–A Research Agenda for Information Systems.*

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Berners-lee, T., & Hara, K. O. (2013). *The read – write Linked Data Web Subject Areas :*

Bies, R. J., & Culnan, M. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, *59*(2), 323–342. http://www.blackwell-synergy.com/doi/abs/10.1111/1540-4560.00067%5Cnhttp://www.blackwell-synergy.com.ezproxy.lib.utexas.edu/doi/full/10.1111/1540-4560.00067

Botterman, M. (2009). for the European Commission Information Society and Media Directorte General. *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*.

Chabridon, S., Laborde, R., Desprats, T., Oglaza, A., Marie, P., & Marquez, S. M. (2014). A survey on addressing privacy together with quality of context for context management in the Internet of Things. *Annales Des Telecommunications/Annals of Telecommunications*, *69*(1–2), 47–62. https://doi.org/10.1007/s12243-013-0387-2

Chatterjee, S. (2020). Factors Impacting Behavioral Intention of Users to Adopt IoT In India: From Security and Privacy Perspective. *International Journal of Information Security and Privacy (IJISP)*, *14*(4), 92–112.

Cusumano, M., & Goeldi, A. (2013). New businesses and new business models. *The Oxford Handbook of Internet*, 239–261.

Danezis, G., & Gürses, S. (2010). A critical review of 10 years of Privacy Technology. *Surveill. Cult. A Glob. Surveill. Soc.*, 1–16.

Domingo, M. C. (2012). An overview of the internet of underwater things. *Journal of Network and Computer Applications*, *35*(6), 1879–1890. https://doi.org/10.1016/j.jnca.2012.07.012

Donaldson, T., & Walsh, J. P. (2015). Toward a theory of business. *Research in Organizational Behavior*, *35*, 181–207. https://doi.org/10.1016/j.riob.2015.10.002

dos Direitos Humanos, O. N. U. D. U. (2016). Disponível em. *Acesso Em*, *5*. https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf

Dutton, W. H., & William, H. D. (2014). Putting things to work: social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. https://doi.org/10.1108/info-09-2013-0047

Eurich, M., Oertel, N., & Boutellier, R. (2010). The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain. *Electronic Commerce Research*, *10*(3), 423–440. https://doi.org/10.1007/s10660-010-9062-0

Gama, M. R., & Santos, C. C. (2019). Capital informacional das comunidades sociais virtuais como suporte a gestão de MPE's. *Ciência Da Informação Em Revista*, *6*(1), 58. https://doi.org/10.28998/cirev.2019v6n1d

Gerami, M., & Sarihi, S. (2020). The impacts of Internet of Things (IOT) in Supply Chain Management. *JOURNAL OF MANAGEMENT AND ACCOUNTING STUDIES*, *8*(3).

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Hassan, M., Jincai, C., Iftekhar, A., & Cui, X. (2020). Future of the Internet of Things Emerging with Blockchain and Smart Contracts. *Future*, *11*(6).

Hutchison, D., & Mitchell, J. C. (1973). Lecture Notes in Computer Science. In *Lecture Notes in Computer Science* (Vol. 9, Issue 3). https://doi.org/10.1016/0020-7101(78)90038-7

Ju, H., Chen, Y., & CB, S. (2020). Energy optimised IoT assisted multiple fuzzy aggravated energy scheduling approach for smart scheduling systems. *Enterprise Information Systems*, 1–15.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Matthias, K., Roalter, L., & Michahelles, F (2010). Things that twitter: social networks and the internet of things. *What Can the Internet of Things Do for the Citizen (CIoT) Workshop at The Eighth International Conference on Pervasive Computing (Pervasive 2010)*. http://www.eislab.net/publications/2010/ThingsThatTwitter_preprint.pdf

Krause, M., & Hochstatter, I. (2005). *Challenges in Modelling and Using Quality of Context (QoC) BT - Mobility Aware Technologies and Applications* (T. Magedanz, A. Karmouch, S. Pierre, & I. Venieris (eds.); pp. 324–333). Springer Berlin Heidelberg.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259.

Maati, B., & Saidouni, D. E. (2020). CIoTAS protocol: CloudIoT available services protocol through autonomic computing against distributed denial of services attacks. *Journal of Ambient Intelligence and Humanized Computing*, 1–30.

Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. *Business Ethics Quarterly*, *30*(1), 65–96. https://doi.org/10.1017/beq.2019.24

Marx, G. T. (2001). Murky conceptual waters: The public and the private. *Ethics and Information Technology*, *3*(3), 157–169. https://doi.org/10.1023/A:1012456832336

Meirelles, F. de S. (2020). *31ª Pesquisa Anual do Uso de TI*. https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados_0.pdf

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications

and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Palomino, H. J. A., Orjuela, S., & Acevedo, C. (2020). *The Internet of Things IoT, a new ecosystem in an interconnected world: Bibliometric Analysis of 2009-2018*.

Pamplona Filho, R. (2014). LEI Nº 12.965, DE 23 ABRIL DE 2014. *Direito UNIFACS–Debate Virtual*, 167.

Paul, B. (2015). The next digital gold rush: how the internet of things will create liquid, transparent markets. *Strategy & Leadership*, *43*(1), 36–41. https://doi.org/10.1108/SL-11-2014-0094

Peoples, C., Parr, G., McClean, S., Scotney, B., & Morrow, P. (2013). Performance evaluation of green data centre management supporting sustainable growth of the internet of things. *Simulation Modelling Practice and Theory*, *34*, 221–242. https://doi.org/10.1016/j.simpat.2012.12.008

Prakash, C., & Saini, R. K. (2020). A Model on IoT Security Method and Protocols for IoT Security Layers. In *Mobile Radio Communications and 5G Networks* (pp. 771–780). Springer.

Santos, C. C. (2015). Investimentos em capacitação empresarial como base para implementação de inovações nas EPP: uma análise da cadeia de metal mecânica em Aracaju. *Revista Brasileira de Administração Científica*, *6*(1), 186–196.

Santos, C. C., & Sales, J. D. A. (2018). Internet of things: is there a new technological position? *International Journal of Innovation*, *6*(3), 287–297. https://doi.org/10.5585/iji.v6i3.178

Santos, C. C., Ufs, P., Sales, J., & Ufs, P. (2015). O Desafio da Privacidade na Internet das coisas - The Challenge of Privacy on the Internet of Things. *Computer Networks*, *13*(1), 212. https://doi.org/10.1145/2966986.2967034

Saxby, S. (2015). 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 and Security Review*, *31*(2), 163–180. https://doi.org/10.1016/j.clsr.2015.01.011

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477–564. https://doi.org/10.5771/0943-7444-2016-4-285

Solove, D. J. (2008). Privacy: A Concept in Disarray Privacy. *Understanding Privacy*, *May*, 1–11. https://doi.org/10.1191/0969733006nej901oa

Steventon, Alan; Wriht, S. (2010). Intelligent spaces: The application of pervasive ICT. *Springer Science & Business Media*.

Sun, Z., & Badi, S. (2020). Evaluating the Impacts of IoT Implementation on Inter-organisational Value Co-creation in the Chinese Construction Industry. *European, Mediterranean, and Middle Eastern Conference on Information Systems*, 698–714.

Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2020). Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science*, *48*(1), 43–63. https://doi.org/10.1007/s11747-019-00704-3

Turchet, L., Fazekas, G., Lagrange, M., Ghadikolaei, H. S., & Fischione, C. (2020). The Internet of Audio Things: state-of-the-art, vision, and challenges. *IEEE Internet of Things Journal*.

Valéry, N. (2012). Welcome to the Thingternet: Things, Rather than People, are About to Become the Biggest Users of the Internet. *The Economist*, 21.

Vasseur, J., Agarwal, N., Hui, J., Shelby, Z., Bertrand, P., & Cedric, C. (2011). *RPL: The IP routing protocol designed for low power and lossy networks Internet Protocol for Smart Objects (IPSO) Alliance*. *April*, 20. http://www.ipso-alliance.org/wp-content/media/rpl.pdf

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law and*

Security Review, *26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., & Borriello, G. (2009). Building the internet of things using RFID: The RFID ecosystem experience. *IEEE Internet Computing*, *13*(3), 48–55. https://doi.org/10.1109/MIC.2009.52

Zhu, Y., Cambou, B., Hely, D., & Assiri, S. (2020). Extended Protocol Using Keyless Encryption Based on Memristors. *Science and Information Conference*, 494–510.

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's INTRAnet of things to a future INTERnet of things: A wireless- and mobility-related view. *IEEE Wireless Communications*, *17*(6), 44–51. https://doi.org/10.1109/MWC.2010.5675777