REVISTA DE TECNOLOGIA APLICADA (RTA)
v.12, n.1, Jan-Abr 2023, p. 68-85.
ISSN: 2237-3713

http://dx.doi.org/10.48005/2237-3713rta2023v12n1p6885

# Internet das coisas: a vulnerabilidade do consumidor no compartilhamento de dados*

## *Internet of things: the consumer vulnerability in data sharing*

**Herlane Chaves Paz**
Universidade Federal de Pernambuco - UFPE
herlanepaz@hotmail.com

**Ana Carolina Vitor**
Pontifícia Universidade Católica de Minas Gerais - PUC MINAS GERAIS
carolinavitor.marketing@gmail.com

**Luiz Fernando Camargo**
Universidade Estadual de Maringá – UEM
luizfernando.camargo@hotmail.com

**Renata Francisco Baldanza**
Universidade Federal da Paraíba - UFPB
renatabaldanza@gmail.com

**Resumo**
A Internet das Coisas (IoT) se faz presente em *smartphones*, *tablets*, *wearable*s, e outros aparelhos que, conectados, passam a fazer parte das nossas vidas. Os benefícios relacionadas à IoT são muitos, porém, surgem questionamentos em relação ao que pode ser feito com esses dados coletados. A LGPD veio para mitigar esses danos e garantir uma maior segurança digital, mas, será que os consumidores estão cientes dos seus direitos e do que acontece quando utilizam dispositivos de IoT? Este artigo tem como objetivo identificar se os consumidores estão cientes dos seus direitos e do que acontece com seus dados pessoais quando utilizam dispositivos de IoT, como também, a percepção desses usuários sobre o compartilhamento de seus dados pelas empresas. Na metodologia foi utilizada abordagem exploratória e descritiva com entrevistas de roteiro semiestruturado. Foi possível constatar que nem sempre está claro para consumidores as implicações, os dados coletados e sua finalidade, bem como o entendimento dos seus direitos garantidos pela LGPD.

**Palavras-chave:** Internet das Coisas (IoT). Lei Geral de Proteção de Dados (LGPD). Comportamento do consumidor. Vulnerábilidade.

**Abstract**
The Internet of Things (IoT) is present in smartphones, tablets, wearables, and other devices that, when connected, become part of our lives. The benefits related to IoT are many, however, questions arise regarding what can be done with this collected data. LGPD came to mitigate this damage and ensure greater digital security, but are consumers aware of their rights and what happens when they use IoT devices? This article aims to identify whether consumers are aware of their rights and what happens to their personal data when using IoT devices, as well as the perception of these users about the sharing of their data by companies. In the methodology, an exploratory and descriptive approach was used with semi-structured

* Received 28 May 2023; accepted in 28 Juny 2023; published online 28 July 2023.

interviews. It was possible to verify that it is not always clear to consumers the implications, the data collected and its purpose, as well as the understanding of their rights guaranteed by the LGPD.

**Keywords:** Internet of Things (IoT), General Data Protection Law (LGPD), Consumer behavior. Vulnerability

## 1 Introdução

A tecnologia se faz cada vez mais presente no cotidiano da sociedade contemporânea. No Brasil, 83% domicílios possuíam internet conforme dados da última pesquisa CETIC – TIC Domicílios. Assim como a conexão aumentou nas residências brasileiras, os principais aparelhos utilizados para acessar a rede são celulares, Microcomputadores, Televisão e Tablets (IBGEeduca, 2019; CETIC, 2022).

A busca por equipamentos que possuem esses recursos de conexão à internet vem apresentando um crescimento, como é o caso dos televisores, que segundo IBGEeduca (2019), em 2018, 23,1% dos televisores eram utilizados para acessar a internet, e em 2019, esse número cresceu 31,9%.

No momento em que a Internet das Coisas (IoT), *smartphones, tablets wearabl*es, brinquedos, eletrodomésticos e outros aparelhos conectados passam a fazer parte das nossas vidas, nós abrimos e conectamos os diversos momentos de nossas vidas. Com isso, nós disponibilizamos nossos dados *online*, permitindo a criação e o compartilhamento de diversos dados, por meio de redes sem fio, por identificação via radiofrequência ou, ainda, por outras tecnologias associadas à IoT.

As tecnologias relacionadas à IoT trazem um grande potencial de melhorar a vida das pessoas e a relação delas com as empresas, enquanto consumidores. Apesar destes benefícios, surgem questionamentos em relação ao que pode ser feito com os dados coletados advindos destes usos, como também quanto à constante vigilância digital dos seus usuários - aspectos que podem levar à perda da privacidade dos seus utilizadores.

Em tempo, vale lembrar que algumas formas usuais cujos consumidores deixam dados na rede se dá não somente quando ele efetiva uma compra via *m-commerce* ou *e-commerce*, mas, também, com outros simples acessos como visualização em sites e blogs, consumo de conteúdo na rede, músicas e vídeos, dentre outras inúmeras possibilidades. Entretanto, a medida certa da consciência de que estes indivíduos deixam rastros para *big data* e *small data* (respectivamente, em uma síntese, dados maiores, normalmente tralhados quantitativamente por algoritmos e dados menores, podendo ser trabalhados qualitativamente pelas organizações) mesmo sem efetivar compras ainda é obscura.

Concomitante a esta realidade, no Brasil, foi criada a Lei Geral de Proteção de Dados – a LGPD 13.709 bem como o Plano Nacional de Internet das Coisas n. 9.854 - com vigências amplas a partir de 2019 (GOV.BR, 2022). Porém, a questão da pesquisa que se segue é até que ponto os usuários consumidores que se utilizam destas tecnologias estão cientes dos seus direitos com relação aos dados coletados na rede e, principalmente, do que acontece quando utilizam dispositivos de IoT no que se refere à exposição destes rastros e como isso potencialmente poderá determinar uma vulnerabilidade deste consumidor sob este aspecto.

Esta crescente utilização de artefatos de IoT pelas pessoas traz à tona a necessidade de se entender o quanto os seus usuários conhecem sobre o acesso e uso dos seus dados pelas empresas. Academicamente, é mister que os consumidores conheçam mais sobre esses

aspectos, para que façam escolhas de consumo de artefatos ou utilizem as tecnologias de IoT mais conscientes de tudo que entregam na rede e às organizações. Todavia, no Brasil, são muito escassas ainda pesquisas sobre as relações entre vulnerabilidade do consumidor, Internet das Coisas e Dados virtuais (que serão trabalhados via *Big data e Small data*) que são lançados na rede pelos próprios consumidores, muitas vezes sem total consciência e/ou permissão.

Desta forma, esse artigo tem como objetivo analisar se os consumidores estão cientes de como seus rastros digitais com seus dados pessoais e de outra natureza são captados e potencialmente utilizados quando utilizam dispositivos de IoT, a percepção desses usuários sobre o compartilhamento de seus dados pelas empresas e dos seus direitos atuais que potencialmente impactam na vulnerabilidade dos mesmos quando utilizam tais tecnologias deliberadamente sem compreensão de todo o contexto adiante.

Para isto, o estudo foi dividido da seguinte forma: no primeiro momento, a construção teórica, em que busca apresentar a definição de IoT, seus desdobramentos e seu impacto nos usuários, a vulnerabilidade dos usuários e também o acesso a LGPD. No segundo momento, empírico, serão apresentados os dados com base na metodologia qualitativa e quantitativa, a discussão e os resultados alcançados.

Ao final deste estudo, foi possível constatar que a IoT está cada vez mais presente na vida dos usuários, porém, nem sempre está claro para eles as implicações, ou seja, os dados coletados e sua finalidade, bem como o entendimento dos seus direitos garantidos pela LGPD, dados estes que serão melhor elucidados adiante.

## 2 Fundamentação Teórica

### 2.1 Internet das Coisas – IoT: perspectivas contemporâneas

Como consequência da fusão entre as indústrias da computação e telecomunicações, a ciência da computação junto com as interfaces de comunicação fixas ou móveis, está hoje formando redes de computação ubíqua. Essas redes têm a característica de conectar não apenas humanos a humanos, mas humanos a objetos e objetos a objetos na qual chamamos de “A Internet das Coisas” (SANTAELLA *et al.*, 2018; HAMMONS; KOVAC, 2019). Diante disso, alguns especialistas argumentam que a Internet das Coisas é a maior inovação em comunicação desde a Web (VALÉRY, 2012; LI *et al*., 2014; DUTTON, 2014).

O termo Internet das Coisas surgiu em 1999 quando, em uma palestra, Kevin Ashton explicava o potencial de uso das radiofrequências, RFID, em 1999 (ASHTON, 2009). Apesar da IoT ter surgido em 1999, vários fatores que compõem o posicionamento tecnológico da Internet das Coisas, estão sendo combinados de novas formas de conectividade sem fio, sensores, dispositivos de captura e tecnologias (DUTTON, 2014). Que para o autor, a próxima grande inovação para a sociedade moderna será a implementação total da Internet das Coisas (DUTTON, 2014).

Segundo Li *et al*. (2014), a IoT está voltada para as aplicações tecnológicas, para as relações estabelecidas entre pessoa-coisa, coisa-pessoa e entre coisa-coisa, o ambiente de comunicação inteligente que consiste em pessoas e coisas sendo configuradas. Já segundo Leite *et al.* (2017), a Internet das Coisas pode ser considerada como uma nova onda tecnológica que criou uma fronteira de conexão do mundo com pessoas, computadores, dispositivos (objetos/coisas), ambientes e objetos virtuais, capazes de se conectarem e interagirem entre si.

Logo, com a popularização desses objetos e aplicações desse paradigma nas mais diferentes atividades humanas, torna-se necessário revisar os procedimentos de segurança associados ao uso dessas implementações (PAUFERRO; PAIVA; LESSA, 2020). Ainda segundo os autores, percebe-se que com aplicações tradicionais para a internet, as aplicações em IoT envolvem a utilização de dados e informações confidenciais e sensíveis de usuários ou de qualquer máquina que esteja aplicada àquele contexto. Com isso, percebe-se a importância de se garantir a segurança da informação que envolvam dados pessoais e/ou dados de empresas, E essa garantia e a falta de conhecimento podem ser um dos fatores que levam a vulnerabilidade do consumidor.

Nesta direção, Rezende *et al*. (2021) destacam que com a rápida expansão da IoT, abriram-se novas e diversificadas perspectivas de usos dessas tecnologias incluindo-se, por exemplo, *smart cities*, *smart grids* dentre outras aplicações. Os autores afirmam, portanto, que estamos diante de um campo multidisciplinar em que a adequada apresentação do conhecimento desses desdobramentos, incluindo-se consumidores, se torna imprescindível. Destarte, propõem a discussão do emprego de ontologias para abordagem destes cenários, que poderão servir tanto para as organizações quanto para maior conscientização do usuário final que consume nos ambientes de IoT.

Assim sendo, sendo a IoT um novo marco na economia digital segundo a perspectiva econômica, pode ficar fora de controle se não for padronizada nos próximos anos (SANTOS; SALES, 2018). Com isso potencialmente aumentam-se problemas relativos às questões relacionadas à privacidade do usuário, proteção de dados e outras questões sociais ligadas a sensores, gerando vulnerabilidade dos consumidores. O conhecimento ontológico, das ferramentas, dos usos algoritmos, de seus direitos e das próprias leis que cercam atualmente estas questões no Brasil como a Lei Geral de Proteção de Dados pode trazer maior probabilidade de consumo consciente dessas tecnologias e recursos, foco central da discussão deste estudo.

## 2.2 Vulnerabilidade do consumidor usuário

Segundo Merabet *et al.* (2021), vulnerabilidade pode ser entendida como uma condição desfavorável, ou seja, alguma fragilidade que coloca o indivíduo em situação de inferioridade. A conceituação da vulnerabilidade é importante porque envolve o bem-estar do consumidor, bem como as respostas das empresas, políticas e da sociedade ao mal-estar do consumidor. O que há em comum entre as pesquisas sobre Vulnerabilidade do Consumidor[1] (VC) é a frequente relação entre vulnerabilidade e desvantagem, embora nem todos aqueles em desvantagem experimentem vulnerabilidades e pessoas sem desvantagens, também percebidas, possam experimentar a vulnerabilidade (BAKER; GENTRY; RITTENBURG, 2005; MERABET *et al.*, 2021).

Silva *et al.*, (2021) afirmam que, pela ótica do Direito, área onde surgiram os primeiros trabalhos sobre o tema, o entendimento da Vulnerabilidade do Consumidor é particularmente importante para que possam ser garantidos direitos iguais para todo e qualquer indivíduo que precise de proteção diferenciada.

É importante destacar que pelo Código de Defesa do Consumidor (BRASIL, 1990), dentre os tipos de VC, encontram-se a vulnerabilidade jurídica (falta de conhecimento jurídico que permita ao consumidor entender as consequências jurídicas dos seus atos) e a

[1] Nesse artigo, entende-se consumidor e usuário como sinônimos.

vulnerabilidade informacional ou técnica (a qual advém da ausência da informação prestada, não permitindo plena compreensão pelo consumidor). Portanto, a vulnerabilidade deste consumidor é característica intrínseca das relações de consumo, seja ele de bens, serviços ou qualquer outro produto passível da troca mercadológica (SOUZA; ALVES, 2020; LEHFELD *et al.*, 2021).

Isso posto, um estudo desenvolvido pela Boa Vista SCPC (LÚLIO, 2018) mostrou que 67% dos brasileiros desconhecem ou conhecem muito pouco sobre seus direitos enquanto consumidores e não acreditam que as empresas, nas relações de consumo, forneçam todas as informações que eles deveriam saber. Sendo assim, pode-se compreender as suas vulnerabilidades jurídica e informacional, especialmente quando focamos nos usuários de artefatos de IoT.

Em consideração a isso, percebe-se ainda a necessidade de pesquisas mais abrangentes sobre a vulnerabilidade, porque mercado e consumo podem ser simultaneamente fonte de conflitos, riscos, vulnerabilidade, significado e prazer que afetam diversos públicos – mais enfaticamente nos usuários com mais artefatos conectados entre si.

Isso, principalmente, levando em conta que a potencial coleta de dados de forma indiscriminada tende a expor esses consumidores ao risco de seus dados serem usados indevidamente, portanto, asseveram Santos *et al.* (2022), a adoção de técnicas para ‘anonimização’ de dados poderia representar um grande avanço na garantia da segurança na Internet, possibilitando ainda, uma maior liberdade aos usuários/consumidores e preservando diversos direitos assegurados constitucionalmente. Diante disso, é nítida a necessidade de uma delimitação da coleta de dados pessoais, bem como a adoção de técnicas que assegurem a privacidade dos usuários, avultam.

Nessa direção, estudiosos de marketing começaram a dar uma maior atenção a VC; e, em 2006, por meio da fundação do movimento Transformative Consumer Research (TCR) pela The Association for Consumer Research - que tem seus estudos definidos como esforços de investigação que lidam com problemas e oportunidades fundamentais com a finalidade de melhorar a qualidade de vida diante dos efeitos do consumo - aumentou consideravelmente o número de trabalhos sobre essa temática (MICK, 2012).

Isso se deve ao surgimento da TCR, objetivando preencher as lacunas e superar a fragmentação no campo da pesquisa em consumo no domínio do bem-estar. Ante ao exposto, segundo Gomes Neto *et al.* (2021), a temática mais explorada pelas pesquisas que adotam as abordagens TCR tem sido a VC.

Diante disso, de acordo com Gomes Neto *et al.*, (2021), consideram-se consumidores vulneráveis, os consumidores em estado de pobreza, com escolhas limitadas, portadores de alguma necessidade especial, entre outros estados de vulnerabilidade, como no caso dos usuários de artefatos de IoT que desconhecem o conteúdo da LGPD e modo de uso de seus dados pessoais pelas empresas.

Perante o exposto, pode-se entender que as práticas das empresas em relação aos usuários de artefatos de IoT, torna-os vulneráveis em relação aos seus dados e põe em risco sua privacidade e intimidade. Pois, de acordo com Efing e Britto (2021), as empresas passaram a esquadrinhar informações pessoais com a finalidade de personalizar o marketing e oferecer maior eficiência nos serviços oferecidos. Nesse sentido, a VC está diretamente vinculada à constatação de que seus dados pessoais são disponibilizados para terceiros em variadas formas. As informações pessoais identificáveis do usuário, seus hábitos de consumo, preferências, entre outras terminam sendo esmiuçadas, comercializadas, sem o conhecimento do usuário.

## 2.3 Lei Geral de Proteção de Dados – LGPD e as nuances da vulnerabilidade

No cenário atual das leis pilares da proteção de dados, podemos citar dois conceitos que elucidam até que ponto há necessidade e gerência governamental em aspectos mercadológicos nas organizações: o '*Privacity by design*' e o '*Privacity by default*'.

Em linhas gerais, o primeiro prevê que projetos de uma organização que envolvam o processamento de dados pessoais devem ser realizados, mantendo a proteção e a privacidade dos dados a cada passo. Isso significa que a organização deve garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida e assegurar a segurança das informações de ponta a ponta. Já o segundo, foco deste estudo por se tratar das questões relacionadas ao consumidor e potenciais vulnerabilidades advindas do consumo em e via rede, determina que, assim que um produto ou serviço for lançado ao público, as configurações mais seguras de privacidade deverão ser aplicadas por padrão e todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas pelo tempo necessário para fornecer o produto ou serviço. (ALVES; PEIXOTO; ROSA, 2021; PRIVACY TECH, 2022).

Diante deste esclarecimento, destacamos o fato de que as pessoas inserem em abundância e de forma incontrolável suas informações em canais digitais todos os dias, sem notar o quanto estão vulneráveis, principalmente quando se trata de consumir no ciberespaço, já que se tornou um espaço a ser explorado fomentando o consumo e o lucro, modificando assim as relações de consumo entre as pessoas e empresas (SIQUEIRA *et al*., 2021).

Em face da constante evolução da tecnologia de informação e de sua utilização, definir uma legislação que regulamente o uso dos meios de comunicação eletrônica é fundamental (WOLKMER, 2013). Entretanto, a falta de punição e o anonimato no meio digital facilitam a violação de direitos, como aponta Norton (2018) que 76% dos adultos brasileiros já foram vítimas de algum tipo de crime digital e chegando a 65% a nível global.

Com a IoT, o número de objetos físicos conectados tem aumentado e com isso permitindo coletar dados para análise e monitoramento, além de permitir automatizar tarefas de acordo com a necessidade do usuário e traçar padrões de comportamento de uso (SINGER, 2012). Neste cenário de hiperconectividade vulnerável a algoritmos e Inteligência Artificial (IA), o direito do consumidor toma novos rumos a fim de proteger e garantir a dignidade dos usuários, com a criação da Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709/2018).

A lei brasileira, em vigor desde 25 de maio de 2018, segue o previsto no Regulamento Geral de Proteção de Dados (GDPR) que é uma lei europeia que conduz toda a coleta e processamento de dados pessoais de indivíduos, visando estabelecer regras de forma a proteger os usuários quando se trata do uso de dados pessoais e regras relacionadas à livre circulação de dados pessoais (TEFFÉ; MEDON, 2020).

A LGPD aborda 65 artigos e inúmeros parágrafos, sendo os principais abordados neste estudo: o uso da informação - especificando qual a finalidade da coleta, tratamento e segurança desses dados, e o acesso à informação - fácil acesso, autorização e revogação dos dados que estão sendo utilizados. Para tanto, busca implementar deveres e responsabilidades a quem coleta dados de seus usuários, de forma a proporcionar a segurança das informações captadas, visando antecipar os riscos de violação à privacidade, como também evitar tratamentos abusivos de informações e vazamentos de dados (TEFFÉ; MEDON, 2020).

Desta forma, verifica-se a importância de se compreender a que ponto os usuários de IoT sabem seus direitos e o quanto fornecem de informações para dispositivos utilizados e todas as nuances supracitadas no decorrer da revisão da literatura e dos argumentos adiante.

## 3 Metodologia

A pesquisa é caracterizada como sendo de nível de aprofundamento/objetivo exploratório e desenvolve metodologia de natureza predominantemente qualitativa, utilizando como instrumento entrevistas com roteiro semiestruturado, dividida em duas etapas: primeiramente foi realizada entrevista presencial e, devido a necessidade das pessoas indicadas pelo método bola de neve, foi disponibilizado no mesmo período, o questionário via internet pela ferramenta do *Google Forms*.

Esta pesquisa situa-se sob o paradigma interpretativista, com enfoque qualitativo, buscando evidenciar a compreensão e interpretação dos próprios sujeitos, uma vez que não considera a existência de uma realidade totalmente objetiva, nem totalmente subjetiva, mas sim, que existe uma interação entre as características de um determinado objeto e entre a compreensão que os seres humanos criam a respeito desse objeto (SACCOL, 2009).

Com o intuito de atender aos objetivos propostos, os sujeitos da pesquisa foram relacionados à segmentação do meio social a ser pesquisado, que precisa ser pertinente ao problema da pesquisa (FRASER; GONDIM, 2004). Com isso, a premissa principal para seleção dos sujeitos foi o uso de IoT, mesmo que os consumidores não consigam identificar com clareza se estão utilizando o IoT, fato esse que poderá ser analisada sua vulnerabilidade.

A escolha pelos sujeitos que colaboraram com a pesquisa se deu por questões de acessibilidade, conveniência e técnicas de "bola de neve", segundo Sampieri, Collado e Lucio (2010), que se identificam os participantes-chave para a pesquisa, e indicam outros participantes para pesquisa.

Foram selecionados 8 indivíduos para participar das entrevistas presenciais entre os dias 01 de janeiro de 2022 e finalizadas no dia 13 de janeiro do mesmo ano. No mesmo período, o instrumento foi disponibilizado via *Google Forms* aos sujeitos pertencentes ao perfil necessário para o estudo, o que abrange atualmente boa parte dos indivíduos que, ao menos, acessam smartphones e utilizam suas ferramentas, recursos e possibilidades na rede, totalizando 27 respondentes. Por se tratar de uma pesquisa de cunho qualitativo, destacou-se que a coleta cessou quando observado a saturação dos dados nas respostas e a ausência, após um certo número de entrevistados, de informações significativas para além das coletadas conforme previa o roteiro semiestruturado.

As entrevistas realizadas de forma presencial foram feitas para acompanhar as reações dos participantes diante dos questionamentos realizados. Dessa forma foram respeitadas as questões éticas envolvidas na pesquisa, também foram solicitadas autorização dos seus respectivos participantes, com documento assinado pelos mesmos autorizando a realização da entrevista, a gravação da mesma e a transcrição de tudo que foi conversado e registrado em áudios. Do mesmo modo, via *Google Forms* também foram respeitadas as questões éticas envolvidas na pesquisa, e solicitadas autorização dos seus respectivos participantes.

O objetivo do estudo também foi informado a todos os participantes durante a entrevista e, para manter a postura ética, os nomes dos entrevistados não aparecem no trabalho, são usados apenas E1 (entrevista 1), E2 (entrevista 2), e assim sucessivamente, para identificar os participantes. Dos sujeitos, E1 ao E8 foram os entrevistados pessoalmente e E9 ao E35 foram os entrevistados via *Google Forms*.

Em tempo, é mister ressaltar que foi utilizada uma pergunta filtro que determinava se "o participante possui o hábito de usar a internet pelo celular ou aparelhos que se conectam por

rede", visto que a vulnerabilidade ao compartilhamento de dados só poderia ser observada no uso de redes

O quadro 1 ilustra o perfil dos entrevistados pessoalmente que fizeram parte da coleta de dados da pesquisa:

**Quadro 1** - Perfil dos entrevistados no formato presencial.

| Nome | Gênero | Idade (faixa etária) | Cidade |
|---|---|---|---|
| E1 | Feminino | De 36 a 45 anos | Teresina |
| E2 | Feminino | De 36 a 45 anos | João pessoa |
| E3 | Feminino | De 25 a 35 anos | Cambé |
| E4 | Masculino | De 25 a 35 anos | Londrina |
| E5 | Feminino | De 18 a 24 anos | Recife |
| E6 | Feminino | De 46 a 56 anos | Recife |
| E7 | Masculino | De 36 a 45 anos | João pessoa |
| E8 | Feminino | De 25 a 35 anos | Minas Gerais |

**Fonte:** Elaborado pelos autores, 2022.

O quadro 2 ilustra o perfil dos entrevistados via *Google Forms* que fizeram parte da coleta de dados da pesquisa:

Foram entrevistados 27 participantes. Posto isso, traçamos as características descritivas dos participantes apontadas na Tabela 1, com o n=27:

**Quadro 2** - Perfil dos entrevistados no formato remoto.

| Nome | Gênero | Idade (faixa etária) | Cidade |
|---|---|---|---|
| E9 | Feminino | De 25 a 35 anos | Piauí |
| E10 | Feminino | De 18 a 24 anos | Minas Gerais |
| E11 | Feminino | De 18 a 24 anos | Paraná |
| E12 | Feminino | De 18 a 24 anos | Paraná |
| E13 | Masculino | De 36 a 45 anos | Paraná |
| E14 | Feminino | De 46 a 56 anos | Pernambuco |
| E15 | Feminino | De 57 a 65 anos | Pernambuco |
| E16 | Masculino | De 25 a 35 anos | Santa Catarina |

| | | | |
|---|---|---|---|
| E17 | Feminino | De 46 a 56 anos | Pernambuco |
| E18 | Feminino | De 46 a 56 anos | Pernambuco |
| E19 | Feminino | De 57 a 65 anos | Pernambuco |
| E20 | Feminino | De 46 a 56 anos | Pernambuco |
| E21 | Feminino | De 18 a 24 anos | Paraná |
| E22 | Feminino | De 46 a 56 anos | Pernambuco |
| E23 | Feminino | De 46 a 56 anos | Paraná |
| E24 | Feminino | De 18 a 24 anos | Paraná |
| E24 | Feminino | De 18 a 24 anos | Paraná |
| E26 | Feminino | De 18 a 24 anos | Paraná |
| E27 | Masculino | De 36 a 45 anos | Paraná |
| E28 | Feminino | De 46 a 56 anos | Pernambuco |
| E29 | Feminino | De 25 a 35 anos | Minas Gerais |
| E30 | Feminino | De 46 a 56 anos | Santa Catarina |
| E31 | Masculino | De 25 a 35 anos | Paraná |
| E32 | Feminino | De 25 a 35 anos | Paraná |
| E33 | Masculino | De 18 a 24 anos | Paraná |
| E34 | Feminino | De 36 a 45 anos | Paraná |
| E35 | Masculino | A partir de 66 anos | Pernambuco |

**Fonte:** Elaborado pelos autores (2022).

A técnica de coleta de dados que melhor se adequou ao contexto e objetivos traçados foi a entrevista, a partir de um roteiro semiestruturado, pois permitiu entender a percepção dos sujeitos sobre o tema pesquisado. Ela é também é adequada para a obtenção de informações acerca do que as pessoas sabem, creem, esperam e desejam, assim como suas razões para cada resposta. Conforme Gil (2009), a entrevista é uma das técnicas de coleta de dados mais utilizadas nas pesquisas sociais.

Os dados foram analisados utilizando a técnica de análise de conteúdo, conforme Bardin (2011), que trabalha a palavra, a prática da língua realizada por emissores identificáveis. Após a coleta de dados, foi realizada a categorização teórica dos resultados, buscando interpretar os dados, justificando a separação deles nas categorias que o instrumento prevê (FLICK, 2009).

## 4. Resultados e Discussão

### 4.1 Categoria 1: Nível de conhecimento Internet das Coisas – IoT: o que é e suas aplicações

A Internet das Coisas é considerada uma nova onda tecnológica que criou uma fronteira de conexão do mundo com pessoas, computadores, dispositivos (objetos/coisas), ambientes e objetos virtuais, capazes de se conectarem e interagirem entre si (LEITE *et al.*, 2017).

Neste sentido, o primeiro tópico do estudo buscou indagar se os participantes sabem ou já ouviram falar de Internet das Coisas e saberiam dar algum exemplo da sua aplicação. Assim como se acreditam que a Internet das Coisas pode ser utilizada por organizações como formas de promoção e comunicação com o consumidor.

> **E2:** "SIM já ouvi falar e tenho Siri, Alexia. A Internet das Coisas é uma evolução definitiva e sem volta, pode ser utilizada por perfis individuais e por organizações também. A partir do momento em que os consumidores adquirem produtos que detêm essa tecnologia, todas as suas funções podem vir carregadas de informações de promoção e comunicação."

> **E3:** "Sim! Eu já ouvi falar e eu conheço algumas aplicações. Por exemplo, eu acho que uma ferramenta muito interessante é a possiblidade de você monitorar equipamentos que estão na sua casa, mesmo você não estando na sua casa. Como é o caso, o que eu faço uso, que é o controle da televisão, o tempo de funcionamento da televisão, o horário que ela foi ligada ou desligada, mesmo eu não estando em casa, eu sou avisado no celular quando isso acontece, quando a tv é ligada e quando a tv é desligada. Além dessa aplicação, conheço outras também muito interessante, que eu acho, é as fechaduras eletrônicas no meu condomínio tem um vizinho que tem isso, então ele tem uma fechadura que é conectada com a internet e ele consegue saber pelo celular dele caso alguém tenha entrado, quem foi que entrou pelo código que foi digitado, ou pela digital da pessoa que foi passada ali na porta, entrando e saindo da casa dele, independente de onde ele esteja."

> **E4:** "Já ouvi falar, principalmente porque, no meu trabalho né? Porque a gente usa soluções que conectam, no nosso caso lá, veículos à internet e aí eu conheço por conta disso. Mas eu sei que tem outras aplicações de usar, conectar coisas à internet, capturar dados e informações das coisas, desde coisas banais, tipo, uma vez eu vi, eu acho que era pente de cabelo, pra acompanhar, tipo umas coisas aleatórias, até coisas que tem mais uso assim. Eu já vi lixo também, pra você acompanhar se está cheio ou vazio, pra você trocar o saco, umas coisas assim."

> **E9-** "Já ouvi falar, mas não entendo bem."

> **E10-** “Nunca ouvi falar.”

As respostas corroboram com os dados descritos no parágrafo acima, tendo em vista que alguns dos sujeitos demonstraram usar bastante a Internet das Coisas. No entanto, nota-se que há ainda várias pessoas que não possuem conhecimento sobre o assunto, muito menos identificam aspectos de Internet das Coisas no dia a dia. Neste sentido, havendo um desconhecimento por parte das pessoas sobre IoT e suas várias formas de aplicação, isso acarreta, consequentemente, em uma falta de consciência da potencialidade da Internet das Coisas.

Quanto aos respondentes pelo *Google Forms* para saber se o tema Internet das Coisas era de conhecimento dos entrevistados, perguntou-se se sabiam ou já tinham ciência do assunto e 13 participantes disseram que sim, 12 que não sabiam o que era.

Buscando aprofundar no quanto conheciam sobre o tema, os entrevistados foram questionados se saberiam dar algum exemplo em que a IoT é utilizada e entre os que disseram conhecer a IoT obtivemos as respostas:

> **E12-** “Com objetivos conectados, exemplo televisão, casas com automação, recentemente ar condicionado, entre outros.”

> **E13-** “Com objetivos conectados, exemplo televisão, casas com automação, recentemente ar condicionado, entre outros.”

Ainda sobre o nível de conhecimento, na pergunta se os participantes sabem quais dados estão sendo coletados?

> **E4:** “Não completamente, mas, nossa deve pegar muita coisa, hábito de consumo, padrão de consumo de informação, hábitos, tipo horários que mais uso tais aplicativos, meu comportamento dentro do celular, voz, tenho certeza absoluta que pega, só de ver as coisas né, que acaba aparecendo, sugerindo. Eu acho que é isso aí, sem contar os dados pessoais, né? Que a gente acaba colocando ali, CPF, nossa! Celular e tal... deve ter a rodo aí.”

Conforme apontam Chouk e Mani (2016) aqueles que não tem consciência de como controlar o uso de tecnologias podem desenvolver alguma dependência tecnológica, os autores alertam que ao ter contato com esse tipo de tecnologia, o consumidor torna-se potencialmente vulnerável porque se expõe a riscos relacionados ao gerenciamento dos dados (segurança, privacidade), sua saúde (física e psicológica) e suas expectativas em relação ao objeto (desempenho e financeiro).

### 4.2 Categoria 2: Vulnerabilidade dos usuários

Após analisar qual o nível de conhecimento dos consumidores com relação à IoT, esta categoria objetivou entender a vulnerabilidade dos usuários.

A vulnerabilidade pode ser entendida segundo Merabet *et al.* (2021), como uma condição desfavorável, ou seja, alguma fragilidade que coloca o indivíduo em situação de inferioridade. Ao serem indagados sobre o acham que pode acontecer com suas informações quando você usa, por exemplo, a Siri, Alexa, etc.? E se acham que as empresas conseguem ter acesso ao que você pesquisa, clica ou fala os participantes responderam:

> **E3:** "eu acho que é um problema, existe um problema de privacidade, mas, normalmente quando você está utilizando essas ferramentas, você cede à permissão para que elas coletem seus dados. Então, o problema é que a gente nem percebe que a gente está cedendo, porque a gente só vai aceitando as formas das, de utilização dessas ferramentas, porque, ou você aceita ou você não usa, né? Então, a opção é não usar."

> **E4:** "Alexa especificamente nunca percebi, mas o celular se falar alguma coisa, algum produto, algum item né, você comentar sobre... isso aparecer, já aconteceu, até de falar em áudio, às vezes, sabe? Depois começa a aparecer as coisas, sabe? Então eu acho que é utilizado sim... deve tá estar lá até nos termos de uso né?"

> **E5:** "As informações coletadas podem ser compartilhadas de forma descontrolada."

> **E30:** "As informações podem ser vendidas."

Quanto ao fato de saber que uma empresa tem acesso a diversas informações pessoais suas, como seus hábitos de consumo, sua localização, ao que você pesquisa, clica ou fala, como eles se sentem:

> **E4:** "Fico meio receoso, mas ao mesmo tempo você fica habituado a aquilo fazer parte do seu dia a dia e os benefícios que aquilo traz que não afeta no meu comportamento no dia a dia."

> **E11:** "Um pouco sem privacidade, mas por ser da área da comunicação entenderia a necessidade."

> **E12:** "Desconfortável, como se estivesse sendo vigiado."

Diante das respostas percebeu-se uma preocupação, por parte dos participantes, sobre a proteção e segurança dos seus dados, tendo em vista que muitos não se sentem à vontade com o destas tecnologias. Neste sentido, é preciso entender que a Internet das Coisas, ao mesmo tempo em que traz benefícios para a sociedade, também apresenta erros, riscos e impactos negativos (FRAZÃO, 2019).

Quando perguntou aos participantes se quando o uso de aplicativos e objetos conectados entre si, as empresas podem lhe conhecer melhor do que você se conhece e lhe ofertar produtos

e serviços que facilitem a sua vida, que atendam suas necessidades – mas que com isso, suas despesas aumentem. O que eles pensam disso:

> **E3:** "Eu acho que, de certa forma, os anúncios personalizados de acordo com o nosso padrão de consumo e de visitas em *websites*, isso de certa forma facilita, eu acho que, a vida das pessoas na forma de consumir. Então, é muito mais fácil eu receber algo na minha casa do que eu sair em lojas procurando, e às vezes aparece algum anúncio de algum produto que, eu poderia até mesmo ter o interesse, mas não era um produto de extrema necessidade, mas uma vez que aparece num anúncio interessante, a gente acaba comprando."

> **E4: "**Eu acho que é uma forma do capitalismo conseguir colocar mais produtos e aumentar o consumo que é importante para o sistema. Então, pensando friamente em como funciona, eu acho um tanto quanto abusivo."

> **E9:** "Infelizmente não temos muito controlar. Cabe a nós, consumidores, estarmos preparados para não cairmos nas armadilhas do consumismo."

Pelas respostas acima percebeu-se que os consumidores, na maioria das vezes, não se sentem satisfeitos com essas práticas e estratégias. Alguns ainda classificaram como aceitáveis algumas práticas de pesquisar algo e depois receber anúncios sobre isso, mas a maioria entende ser abusiva esse tipo de prática.

### 4.3 Categoria 3: Conhecimento sobre Lei Geral de Proteção de Dados

Com a IoT, o número de objetos físicos conectados tem aumentado e com isso permitindo coletar dados para análise e monitoramento, além de permitir automatizar tarefas de acordo com a necessidade do usuário e traçar padrões de comportamento de uso (SINGER, 2012). Neste cenário conhecer a Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709/2018), é essencial para proteger e garantir a dignidade dos usuários.

Diante disso, ao realizar a pergunta se os usuários sentem segurança ao usar a internet?

> **E4: "**De maneira geral sim! Até porque eu nunca vivenciei nada que tenha colocado, tipo tenha tido um problema em relação a isso. Mas, por exemplo, li hoje em algum lugar, que teve algum vazamento de informação, acho que era de PIX, de informação de cadastro de PIX, alguma coisa assim. Nesses momentos em que eu tenho contato com esse tipo de informação, eu me sinto vulnerável, e quando eu começo a racionalizar o tanto de vezes que eu coloco meu CPF nas coisas, que eu cadastro meu cartão de crédito em aplicativo de comida, em UBER, 99, aí eu começo a ter consciência de tipo... quanto eu tô exposta."

> **E33:** "Não, a internet possui muitas coisas positivas, mas também muito mais coisa negativo, nas camadas mais profundas dela."

Dentre as 35 pessoas que foram ouvidas, apenas 11 não se mostraram seguros ao utilizarem a internet, mas até os que sentem segurança ao usar, apresentou palavras como: medo, invasão, bombardeio, falta de privacidade, dentre outras que se apresentaram de forma muito mais negativa do que positiva. Um fato que chamou atenção foi que apenas 4 usuários já foram vítimas de algum crime digital e quando são indagados se já ouviu falar da Lei Geral de Proteção de Dados? Se sim, o que você pode dizer sobre ela?

> **E4:** "Já! Bom sei que é uma legislação nova, está em vigor desde o ano passado, se não me engano, que coloca algumas regras no uso de dados pessoais, tem a diferença lá né? Dos dados pessoais, dados "sensível", eu não vou saber diferenciar. Mas que impõe algumas regras pro compartilhamento de informações."

> **E13:** "Sim, que é uma evolução tardia da internet, penso que essa lei deveria ter sido criada muito antes, e cada vez mais, adaptar-se a evolução da sociedade e das formas de tratamento dos dados."

Alguns participantes também evidenciaram questões sobre a Lei Geral de Proteção dos Dados. A LGPD foi aprovada em agosto de 2018, com vigência a partir de agosto de 2020 e propõe criar um cenário de segurança jurídica, dados esses evidenciados na LEI Nº 13.709, 2018.

Quando foi perguntado sobre quais são seus direitos amparados pela LGPD? 20 participantes não sabem dos seus direitos e mesmos aqueles que disseram sim para conhecer seus direitos, não souberam responder quais eram seus direitos. Os que sabiam seus direitos responderam:

> **E13:** "As organizações que utilizam seus dados precisam informar quais dados elas vão utilizar e para o que utilizarão seus dados, se para soluções, ou mesmo para comercialização. A lei regulamenta as formas de utilização dos dados."

> **E19:** "Sei por exemplo que as empresas não podem usar seus dados de cadastro pra ficar oferecendo coisas sem autorização".

Nota-se uma preocupação, por parte de alguns participantes, sobre a proteção e segurança dos seus dados, por isso buscam conhecimento. No entanto, a maioria não sabe de seus direitos. Diante disso, a vulnerabilidade dos consumidores em domínios digitais torna-se um grande desafio para a pesquisa em marketing e, consequentemente, para o comportamento do consumidor (NG; WAKENSHAW, 2017).

Portanto, essa falta de conhecimento de seus direitos leva a vulnerabilidade, isso ocorre quando as pessoas sequer conhecem as várias formas de aplicação da IoT e quando não imaginam que os seus dados estão expostos e sendo utilizados para vários fins.

## 5 Considerações Finais

A presente pesquisa teve como objetivo identificar se os consumidores estão cientes dos seus direitos e do que acontece com seus dados pessoais quando utilizam dispositivos de IoT, como também, a percepção desses usuários sobre o compartilhamento de seus dados pelas empresas.

A partir da Internet das Coisas, é possível ter acesso a inúmeros dados dos indivíduos através da conexão não apenas humanos a humanos, mas humanos a objetos e objetos a objetos. Todavia, esses consumidores, em sua maioria, não têm conhecimento dos direitos quanto da exposição dos seus dados e de tudo que as organizações conseguem ter acesso. Ao tomarem conhecimento disso, os participantes se mostraram incomodados e palavras como: invasão, falta de privacidade, medo.

Durante as entrevistas foi possível identificar que alguns conhecem a Internet das Coisas e suas várias formas de aplicação. Entretanto, outros constataram ser uma tecnologia que apenas ouviram falar e não saberiam definir ou citar exemplos da sua aplicação. Neste sentido, vale ressaltar que a utilização de IoT já estão presentes no cotidiano dos indivíduos, e muitas vezes passam despercebidas pela visão dos consumidores que não conseguem ter noção que estão inseridos e que seus dados podem ser coletados e essa falta de conhecimento leva a vulnerabilidade e não entendimento de seus direitos pela LGPD. Por isso, urge a necessidade da elaboração de políticas positivas e assertivas específicas para proteger e orientar os consumidores quando se trata do uso de dados.

Cabe ressaltar que as conclusões deste estudo não são passíveis de generalizações em razão de algumas limitações da pesquisa, como o fato de se tratar de uma pesquisa feita com um pequeno grupo de entrevistados, não cabendo considerá-lo como uma representação do todo. Por se tratar de uma temática derivada da LGPD que é uma lei recente no Brasil e ainda pouco abordada, sugerem-se pesquisas futuras que usem uma amostra probabilística que possa retratar estatisticamente um resultado que aponte a representatividade da população brasileira.

## Referências

ALVES, D.; PEIXOTO, M.; ROSA, T. **Internet das Coisas**: segurança e privacidade dos dados pessoais. Rio de Janeiro: Alta Books, 2021.

ASHTON, K. Essa coisa de 'Internet das Coisas'. **RFiD Journal**, v. 22, n.7, p. 97-114, 2009.

BAKER, S. M., GENTRY, J. W., & RITTENBURG, T. L. Building understanding of the domain of consumer vulnerability. **Journal of Macromarketing,** 25(2), 128-139, 2005.

BARDIN, L. **Análise de conteúdo**. Rio de Janeiro: Edições 70, 2011.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 8 de julho de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-022/2019/lei/l13853.htm>. Acesso em: 11 dez. 2021.

BRASIL. Lei nº 12. 965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 dez. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 dez. 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor - Lei 8078/90. Brasília, DF, 1990. Disponível em: https://presrepublica.jusbrasil.com.br/legislacao/91585/codigo-de-defesa-do-consumidor-lei-8078-90. Acesso em: 10 de jan. 2022

CETIC DOMICÍLIOS 2020. Disponível em: https://cetic.br/media/analises/tic_domicilios_2020_coletiva_imprensa.pdf. Acesso em 20 de abr. 2022.
essa referência é a mesma da outra errada abaixo e foi colocada corretamente na letra

BDUTTON, W. H. Colocando as coisas para funcionar: desafios sociais e políticos para a Internet das Coisas. **Ciência da informação**, v. 16, n. 3, p. 1-21. 2014.

EFING, A.; BRITTO, M. A. A reafirmação dos direitos do consumidor virtual brasileiro e a Lei Geral de Proteção de Dados. **Argumenta Journal Law**, Jacarezinho – PR, Brasil, n. 35, 2021, p. 93-121. 2021.

FLICK, U. Introdução à pesquisa qualitativa. 3 ed. São Paulo/SP: **Artmed**, 2009.

FRASER, M. T. D.; GONDIM, S. M. G. Da fala do outro ao texto negociado: Discussões sobre a entrevista na pesquisa qualitativa. **Paidéia**. v. 14, n. 28, p.139 -152, 2004.

GDPR EU. General Data Protection Regulation (GDPR). [s.d.]c. Disponível em: <https://gdpr.eu/tag/gdpr/>. Acesso em: 11 de dez. 2021.

GLASER B. G., STRAUSS A. L. **The discovery of grounded theory**. New York: Aldine Publishing Company; 1967.

GOMES NETO, M. B.; SILVA, L. N.; LIMA, S.H.O.; GRANGEIRO, R. Análise da Produção Científica sobre Transformative Consumer Research e Transformative Service Research. Jan-Mar 2021 • https://doi.org/10.1590/1984-92302021v28n9604PT. 2021.

Ministério da Economia. Plano Nacional de Internet das Coisas. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/plano-nacional-de-internet-das-coisas. Acesso em: 18 de abr. 2022.

HAMMONS, R. L.; KOVAC, R. J. **Fundamentals of internet of things for non-engineers**. New York: Auerbach Publications, 1. ed., 2019.

Instituto Brasileiro de Geografia e Estatística - IBGEeduca. Matérias especiais, uso de internet, televisão e celular no Brasil. 2022. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html#subtitulo-3. Acesso em: 15 de jan. 2022.

LEHFELD, L. S. SIQUEIRA, O. N.; CONTIN, A. C.; BARUFI, R. B. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. Revista Eletrônica Pesquiseduca, v.13, n.29, 2021.

LEITE, J.R.E.; MARTINS, P.S.; URSINI, E. A Internet das Coisas (IoT): Tecnologias e Aplicações. In: **Brazilian Technology Symposium**, 2017, Campinas - São Paulo. Proceedings [...]. [s. l.: s. n.], 2017. DOI ISSN 2447-8326.

LI, S., DA XU, L., & ZHAO, S. A Internet das Coisas: uma pesquisa. Fronteiras de sistemas de informação, v. 17, n. 2, p. 243-259, 2015.

LULIO, M. 67% dos consumidores conhecem pouco sobre seus direitos (2018).. Disponível em: https://www.consumidormoderno.com.br/2018/03/16/consumidores-conhecem-direitos/. Acesso em: 10 de jan. 2022.

MICK, D. G, PETTIGREW, S., PECHMANN, C & OZANNE, J. L. (2012), "Origins, Qualities, and Envisionments of Transformative Consumer Research," in Transformative Consumer Research for Personal and Collective Well-Being, New York: Routledge, 3-24. Disponível em: https://gates.comm.virginia.edu/dgm9t/Mick%20et%20al.%202012%20Origins,%20Qualities,%20and%20Envisionments%20of%20TCR.pdf . Acesso em: 01 de jan. 2022.

NORTON. Relatório de Crimes Cibernéticos NORTON: O impacto humano. Disponível em: <https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf.> Acesso em: 12 de dez. 2021.

REZENDE, M. V.; MARQUES, R. M.; PARREIRAS, F. S. Utilização de ontologias na avaliação de segurança cibernética na Internet das coisas: uma revisão sistemática de literatura. **Revista Ciência da Informação**. Brasília, v. 50, n. 1, p. 198-216, 2021.

PAUFERRO, G. B. A., DE PAIVA, S. V. F., & LESSA, N. M. IoT: conceitos de segurança de dados e criptografia. **Cogitare**, v. *3*, n. 2, p. 40-52. 2020.

PRIVACY TECH. Privacy by Design e by Default: entenda a diferença - Conceitos que são fundamentais para a proteção de dados dentro das empresas. Disponível em: https://privacytech.com.br/noticias/privacy-by-design-e-by-default-entenda-a-diferenca,322343.jhtml. Acesso em 22 de abr./2022.

SACCOL, A. Z. Um retorno ao básico: compreendendo os paradigmas de pesquisa e sua aplicação na pesquisa em administração. **Revista Adm. UFSM**, Santa Maria, v.2, n.2, p. 250-269, 2009.

SAMPIERI, R. H.; COLLADO C. F.; LUCIO, M. P. B. **Metodologia de la invetsigación**. Mc Graw-Hill, 2010.

SANTAELLA, L., GALA, A., POLICARPO, C., & GAZONI, R. **Desvelando a Internet das Coisas**. Revista GEMInIS, 4(2), 19-32, 2018.

SANTOS, C. C., & SALES, J. D. A.. Internet of things: is there a new technological position?. **International Journal of Innovation: IJI Journal**, v. *6, n.* 3, p. 287-297. 2018.

SANTOS, M.; CERQUEIRA, N.; MENEGHETTI, R. Data anonimization as a guarantee to the right to privacy on the internet of things (Internet of Things-IoT). 2021. Disponível em: file:///C:/Users/PC/Downloads/161-Texto%20do%20artigo-767-1-10-20210103.pdf. Acesso em 19 de abr. 2022.

SILVA, R. O., BARROS, D. F., GOUVEIA, T. M. O., MERABET, D. O. B.. Uma discussão necessária sobre a vulnerabilidade do consumidor: avanços, lacunas e novas perspectivas. **Cad. EBAPE.BR** 19, 2021. https://doi.org/10.1590/1679-395120200026

SINGER, T. Tudo conectado: conceitos e representações da Internet das Coisas. In: **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1–15, 2012.

SIQUEIRA, O. N., CONTIN, A. C., BARUFI, R. B., & DE SOUZA LEHFELD, L. A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, v. 13, n. 29, p. 236-255, 2021.

SOUZA, T. A.; ALVES, S. E. S. A proteção ao consumidor no âmbito do comércio eletrônico:uma análise à luz do princípio da vulnerabilidade. 2020. Disponível em: http://ri.ucsal.br:8080/jspui/bitstream/prefix/626/1/TCCTHAIANESOUZA.pdf. Acesso em: 17 de abr. 2022.

TEFFÉ, C. S; MEDON, F. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **Revista Estudos Institucionais**. v. 6, n. 1, p. 301-333, jan./abr. 2020.

THE ASSOCIATION FOR CONSUMER RESEARCH (2022). Disponível em: https://www.acrwebsite.org/web/tcr/. Acesso em 10 de mar. 2022).

VALÉRY, N. Bem-vindo ao thingternet: as coisas, ao invés das pessoas, estão prestes a se tornar os maiores usuários da Internet. **The Economist**, 21b. 2012.

WOLKMER, A. C. Introdução aos fundamentos de uma teoria geral dos “novos” direitos. Revista Jurídica UNICURITIBA, v. 2, n. 31, p. 121-148, 2013. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/593>. Acesso em: 12 dez. 2021.