



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE ARTES E COMUNICAÇÃO
PROGRAMA DE PÓS GRADUAÇÃO EM DESIGN

Jayne Silva de Oliveira

**DESIGN ÉTICO DE WEARABLES:
Investigando a experiência do usuário sobre ética,
privacidade e segurança em smartwatches**

Recife
2025

JAYNE SILVA DE OLIVEIRA

**DESIGN ÉTICO DE WEARABLES:
Investigando a experiência do usuário sobre ética,
privacidade e segurança em smartwatches**

Dissertação apresentada ao Programa de Pós-Graduação em Design da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestra em Design.

Orientador: João Marcelo Xavier Natário Teixeira

Recife

2025

.Catalogação de Publicação na Fonte. UFPE - Biblioteca Central

Oliveira, Jayne Silva de.

Design ético de wearables: investigando a experiência do usuário sobre ética, privacidade e segurança em smartwatches / Jayne Silva de Oliveira. - Recife, 2025. 109f.: il.

Dissertação (Mestrado) - Universidade Federal de Pernambuco, Centro de Artes e Comunicação, Programa de Pós-Graduação em Design, 2025.

Orientação: João Marcelo Xavier Natário Teixeira.
Inclui referências, apêndices e anexos.

1. Smartwatch; 2. Ética em smartwatch; 3. Percepção do usuário; 4. Segurança e privacidade de dados. I. Teixeira, João Marcelo Xavier Natário. II. Título.

UFPE-Biblioteca Central

JAYNE SILVA DE OLIVEIRA

**“DESIGN ÉTICO DE WEARABLES: INVESTIGANDO A EXPERIÊNCIA DO
USUÁRIO SOBRE ÉTICA, PRIVACIDADE E SEGURANÇA EM
SMARTWATCHES.”**

Dissertação apresentada ao Programa de Pós-Graduação em Design da Universidade Federal de Pernambuco, na área de concentração Planejamento e Contextualização de Artefatos, como requisito parcial para a obtenção do título de Mestra em Design.

Aprovada em: 15/08/2025.

BANCA EXAMINADORA

Prof. Dr. João Marcelo Xavier Natário Teixeira (Orientador)
Universidade Federal de Pernambuco

Prof. Dr. Walter Franklin Marques Correia (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Claudio Roberto Marquette Mauricio (Examinador Externo)
Universidade Estadual do Oeste do Paraná

AGRADECIMENTOS

Para uma menina que fazia pré-vestibular, sonhava com a graduação e tinha medo de não passar, ter chegado até o mestrado e passado por tanta coisa é grandioso demais. E isso tudo eu devo a vocês, minha base, meus pais.

Vocês sempre trabalharam muito, debaixo de sol e chuva, para que pudéssemos ter chegado até aqui e eu reconheço que, sem vocês, não teríamos conseguido. Enfrentaram dificuldades, medos, cansaço, falta de recursos, barreiras de todo tipo. Sempre mantendo a postura, a graciosidade e o incentivo. Vocês são verdadeiros gigantes sobre os quais eu tive o privilégio de me apoiar! Sou muito abençoada e orgulhosa por ser filha de vocês.

Além de vocês, também tenho a honra de contar com o incentivo de outro pelo qual vocês lutaram tanto: o meu irmão. A você, irmãozinho, tenho um agradecimento especial. Você que subiu primeiro na vida e conseguiu enxergar longe, te agradeço por ter me estendido a mão. Por ter guiado o caminho, o melhor possível. Por também ser um incentivador dos meus sonhos e sempre torcer pelo meu melhor.

Por fim, mas não menos importante, também agradeço àquele que encontrei ao longo da vida e que também sempre me apoiou muito. Obrigada meu amor por sempre me ouvir e me lembrar de ter equilíbrio na vida.

Em todos vocês, vejo o quanto Deus é, acima de todos esses cuidados, ainda mais graciosos e bondosos comigo. Ter vocês na minha vida é a prova real e nítida de que Deus me ama e provê mais do que peço e muito mais ainda do que mereço. Obrigada é uma palavra pequena demais para o tamanho da minha gratidão a todos vocês.

"Antes de ser designer, você é um ser humano. Como qualquer outro ser humano no planeta, você faz parte de um contrato social. Ao escolher ser designer você está optando por impactar as pessoas que entram em contato com seu trabalho, podendo ajudá-las ou prejudicá-las com suas ações."

(Monteiro, 2015, p. 19, tradução nossa)

RESUMO

O presente estudo corresponde ao mapeamento das opiniões dos usuários acerca da ética percebida por eles no uso de smartwatches. A preocupação em realizar este estudo vem do fato de que esses dispositivos são projetados para interagir com os usuários cotidianamente, coletando diversas informações pessoais como localização, hábitos de exercício, preferências de navegação, além de informações relacionadas à saúde como qualidade do sono, batimentos cardíacos, entre outros.

Contudo, esses dispositivos possuem diversas vulnerabilidades de segurança e privacidade, o que expõe o usuário a constantes riscos. Por fim, como será visto ao longo do estudo, existem princípios, diretrizes e regulamentações que indicam como deve ser realizada a construção de dispositivos conectados, tendo em vista proteger o usuário. No entanto, tais medidas ainda não são exploradas de forma efetiva.

Por isso, o mapeamento da experiência e nível de confiança desses usuários é importante para endossar o quanto as medidas éticas são fundamentais para a percepção e experiência do usuário, aumentando a aceitação e confiança no dispositivo. Os resultados da pesquisa revelam que, embora os usuários demonstrem algum conhecimento sobre os dados coletados, esse conhecimento é parcial e centrado nas funcionalidades mais visíveis do cotidiano.

Além disso, identificou-se que fatores como escolaridade e faixa etária influenciam diretamente na preocupação com segurança e privacidade, mas que essa preocupação nem sempre acompanha a frequência de uso. Assim, a pesquisa reforça a importância de incorporar princípios éticos no design de tecnologias vestíveis, promovendo maior transparência, acessibilidade da informação e confiança por parte dos usuários.

Palavras-chave: *smartwatch*; ética em *smartwatch*; percepção do usuário; segurança e privacidade de dados.

ABSTRACT

This study aims to map users' opinions regarding the ethics they perceive in the use of smartwatches. The motivation behind conducting this research lies in the fact that these devices are designed to interact with users on a daily basis, collecting a wide range of personal information such as location, exercise habits, browsing preferences, and health-related data, including sleep quality, heart rate, among others.

However, these devices present several security and privacy vulnerabilities, which expose users to constant risks. As will be discussed throughout the study, there are principles, guidelines, and regulations that indicate how connected devices should be designed in order to protect the user. Nevertheless, such measures are still not effectively explored or implemented.

Therefore, mapping users' experiences and their level of trust is important to emphasize how ethical measures are essential to the user's perception and overall experience, increasing both acceptance of and trust in the device. The research findings reveal that, although users demonstrate some awareness of the data being collected, this knowledge is partial and mostly limited to the most visible, everyday functionalities.

Furthermore, the study identified that factors such as education level and age group directly influence concerns about security and privacy; however, such concerns do not always align with the frequency of use. Thus, the research reinforces the importance of incorporating ethical principles into the design of wearable technologies, promoting greater transparency, information accessibility, and user trust.

Keywords: smartwatch; ethics in smartwatch; user perception; privacy and data security.

LISTA DE ILUSTRAÇÕES

FIGURAS

Figura 1 –	Seres informacionais	17
Figura 2 –	Mapa conceitual da pesquisa	19
Figura 3 –	Tópicos a serem discutidos a seguir	21
Figura 4 –	Exemplo da diferença entre dados e informação	22
Figura 5 –	Aceite dos termos e condições	25
Figura 6 –	Classificação dos smartwatches	28
Figura 7 –	Esquema visual que ilustra o tema a ser tratado	33
Figura 8 –	Esquema visual a respeito de todos os conceitos descritos neste capítulo	35
Figura 9 –	Análise do nível de concordância entre os respondentes	56
Figura 10 –	Nuvem de palavras a respeito dos dados coletados pelo dispositivo	65
Figura A1 –	Capa do questionário, explicações gerais e termo de responsabilidade	81
Figura A2 –	Consentimento do participante e filtragem inicial	82
Figura A3 –	Mapeamento das características demográficas do participante	82
Figura A4 –	Continuação das perguntas demográficas	83
Figura A5 –	Questões relacionadas à percepção do usuário a respeito da ética, privacidade e segurança dos smartwatches	84
Figura A6 –	Continuação das questões sobre ética e experiência do usuário	85
Figura A7 –	Questões sobre a experiência do participante com o questionário	86
Figura B1 –	Capa do questionário e breve explicação sobre a pesquisa	87
Figura B2 –	Acesso ao termo de consentimento e autorização do usuário	88
Figura B3 –	Informações demográficas	89
Figura B4 –	Continuação das perguntas demográficas	90

Figura B5 –	Parte final das perguntas demográficas	91
Figura B6 –	Perguntas sobre ética, segurança e privacidade dos usuários	92
Figura B7 –	Continuação das perguntas relacionadas a ética	93
Figura B8 –	Parte final do questionário	94
Figura C1 –	Início do documento	95
Figura C2 –	Objetivos e riscos da pesquisa	96
Figura C3 –	Comentários e considerações	97
Figura C4 –	Aprovação do Comitê	98
Figura D1 –	Termo de Consentimento Livre e Esclarecido - Coleta de Dados Virtual	99
Figura D2 –	Continuação do Termo de Consentimento	100
Figura E1 –	Capa da cartilha	101
Figura E2 –	Informações sobre os autores	102
Figura E3 –	Introdução e Objetivo da cartilha	103
Figura E4 –	Principais riscos identificados	104
Figura E5 –	Recomendações para designers e desenvolvedores	105
Figura E6 –	Continuação das recomendações	106
Figura E7 –	Checklist e conclusão da cartilha	107
Figura E8 –	Referências da cartilha	108
Figura E9 –	Contracapa da cartilha	109

GRÁFICOS

Gráfico 1 –	Distribuição de usuários por motivação de uso	61
Gráfico 2 –	Distribuição da motivação de uso por faixa etária	63
Gráfico 3 –	Relação entre escolaridade vs nível de preocupação	64
Gráfico 4 –	Relação entre frequência de uso vs nível de preocupação	64

QUADROS

Quadro 1 –	Lista de funcionalidades comuns entre os smartwatches	29
Quadro 2 –	Vulnerabilidades de segurança e privacidade encontradas nos smartwatches	30
Quadro 3 –	Publicações analisadas na revisão	42
Quadro 4 –	Pesquisas similares e suas contribuições	52
Quadro 5 –	Relação entre as questões de pesquisa e hipóteses e perguntas elaboradas para o questionário	53

SUMÁRIO

1	INTRODUÇÃO	14
1.1	JUSTIFICATIVA E RELEVÂNCIA	15
1.2	CONTEXTUALIZAÇÃO	16
1.3	OBJETO DE ESTUDO	20
1.4	OBJETIVOS	20
1.4.1	Objetivo Geral	20
1.4.2	Objetivos Específicos	20
2	REFERENCIAL TEÓRICO	21
2.1	DADOS	22
2.1.1	Dados - Definição geral	22
2.1.2	Privacidade e segurança	23
2.1.3	LGPD e suas limitações	25
2.2	SMARTWATCHES	27
2.3	ÉTICA: CONTEXTUALIZAÇÃO E CONCEITOS	32
2.3.1	Ética normativa e deontológica	33
2.3.2	Data ethics e a ética profissional do designer	35
2.3.3	Ética profissional aplicada ao design	37
2.4	DIRETRIZES ÉTICAS E ESTRATÉGIAS DE SEGURANÇA E PRIVACIDADE DOS USUÁRIOS DE WEARABLES	38
2.4.1	Estratégia de Busca e Seleção de Fontes	38
2.4.1.1	Combinações de termos de busca	39
2.4.1.2	Processo de Seleção e Filtragem	39
2.4.2	Validação e Garantia de Confiabilidade	40
2.4.3	Análise de Dados	41
2.4.4	Limitações Metodológicas	41

2.4.5	Resultados	41
2.4.6	Discussão	44
2.5	DESIGN: ÉTICA E EXPERIÊNCIA DO USUÁRIO	45
3	METODOLOGIA	49
4	ELABORAÇÃO DO QUESTIONÁRIO E PESQUISA DE TESTE	51
4.1	ELABORAÇÃO DO QUESTIONÁRIO	51
4.2	RESULTADOS PARCIAIS	54
4.3	CONCLUSÃO DO TESTE E MELHORIAS	56
5	PESQUISA QUALITATIVA	58
6	CONCLUSÃO	65
7	RECOMENDAÇÕES ÉTICAS	67
8	DIFICULDADES E LIMITAÇÕES DA PESQUISA	68
9	TRABALHOS FUTUROS	69
	REFERÊNCIAS	70
	APÊNDICE A - Formulário de teste	80
	APÊNDICE B - Formulário da pesquisa qualitativa	86
	ANEXO A - Parecer do Comitê de Ética	94
	ANEXO B - Termo de Consentimento Livre e Esclarecido - Coleta De Dados Virtual	98
	ANEXO C - Cartilha de boas práticas éticas em smartwatches	101

1. INTRODUÇÃO

Wearable devices, ou dispositivos vestíveis, correspondem a uma categoria de dispositivos que possuem em comum o fato de serem desenvolvidos para o uso no corpo ao longo do dia. Fazem parte dessa categoria aparelhos como anéis, óculos, relógios, que, ao contrário dos acessórios comuns, são considerados inteligentes por possuírem sensores que capturam dados dos seus usuários, além de se conectarem com a internet e com outros dispositivos (GCF Global, 2019).

Atualmente, o mercado de *wearables* passa por uma desaceleração das vendas ao redor do mundo, enquanto no Brasil os números têm voltado a crescer (Laricchia, 2014) (CHANNEL 360, 2023). Dentre os vestíveis mais vendidos no país, lideram os *smartwatches*, os quais são dispositivos que oferecem maior conectividade e praticidade aos usuários (AMAZON, 2024).

Devido a essa capacidade conectiva, esses aparelhos são capazes de coletar, processar e compartilhar uma grande quantidade de dados diariamente sobre seus usuários, o que inclui informações como batimentos cardíacos, monitoramento de sono, localização, entre outros (Salutes, 2021). Essas informações podem ser utilizadas para dar ao próprio usuário *insights* sobre sua saúde, permitindo que ele desenvolva hábitos mais saudáveis (Dados para quê?, 2021).

No entanto, de acordo com Atlam e Wills (2019), esses dispositivos, assim como outros que se configuram como *Internet of Things* (IoT) — ou seja, aparelhos que possuem a capacidade de se conectar com a internet e com outros dispositivos —, contêm diversos desafios éticos como a garantia da segurança dos dados e privacidade dos usuários. Essas questões podem, além de comprometer a experiência do usuário, implicar em impactos sociais de grande escala, como vazamento de dados ou promover risco à vida.

Por causa disso, analisar a ética dos *smartwatches*, bem como a forma como ela é percebida pelos usuários, é importante para garantir que esse produto não só possua um design ético e cause bons impactos sociais, mas também que seja entendido pelos usuários como um aliado social confiável.

Nesse sentido, esse trabalho almeja investigar a experiência dos usuários de *smartwatches* em relação à privacidade e segurança, visando dessa forma contribuir para o design de *wearables* mais éticos e respeitosos.

1.1 JUSTIFICATIVA E RELEVÂNCIA

No cenário atual de hiperconectividade, a captura, o processamento, o armazenamento e o compartilhamento de dados tornaram-se essenciais para a identificação e personalização de experiências, além de facilitarem a tomada de decisões dos usuários (MJV Innovation, 2024).

Nesse contexto, os dispositivos vestíveis, como *smartwatches*, desempenham um papel fundamental. Eles monitoram e coletam dados em tempo real, e se integram a outros dispositivos e plataformas digitais. Essa conectividade contínua permite gerar *insights* valiosos que melhoram a saúde, o bem-estar e a eficiência do usuário, além de expandir as possibilidades de interação e comunicação, tornando as experiências mais dinâmicas e conectadas em todos os aspectos do cotidiano (Globalyo, 2024).

Tendo em vista esse cenário, Luciano Floridi e Taddeo (2016) introduzem o conceito de *data ethics*, no qual se entende que as questões éticas não devem levar em consideração apenas o dispositivo em si, mas principalmente que dados estão sendo coletados, como estão sendo tratados e com quem estão sendo compartilhados. Floridi (2018) reconhece que, embora existam leis como o Regulamento Geral de Proteção de Dados (GDPR), da União Européia, e a Lei de Proteção de Dados Pessoais (LGPD) brasileira, que regulamentam a coleta e manuseio dos dados, bem como apontam as práticas permitidas e não permitidas, é trabalho da discussão ética apontar, dentro do permitido, as **melhores práticas** tendo em vista a responsabilidade social.

Nesse sentido, Roossien, C. C. *et al.* (2021) destacam a necessidade de uma visão holística a respeito do tema, tendo em vista desenvolver um dispositivo ético como um todo. Segundo os autores:

“Até agora, os estudos têm em sua maioria focado em questões éticas no design de novas tecnologias ou questões éticas na implementação de tecnologias existentes (11, 12, 16). Ao

considerar as questões em torno da implementação, as tecnologias são geralmente tomadas como um dado e os valores inerentes ao design não são questionados. Esta situação não faz justiça à realidade: se o design e implementação não reconhecem preocupações éticas e valores pretendidos um do outro, o uso final da tecnologia não refletirá as intenções de ambos os lados”. (tradução nossa)

Sendo assim, esse trabalho mostra-se importante, visto que se propõe a investigar a experiência atual dos usuários de *smartwatches*, bem como suas preocupações com ética, segurança e privacidade, para que profissionais *designers* e desenvolvedores possam conceber dispositivos mais éticos, levando em consideração não só a segurança das informações, como também a percepção e a experiência do usuário.

Por isso, o presente estudo torna-se relevante para a sociedade já que objetiva contribuir para a inovação responsável, à medida que visa contribuir para a responsabilização ética dos profissionais *designers* e desenvolvedores.

1.2 CONTEXTUALIZAÇÃO

Luciano Floridi (2015, *apud* Souza, 2021, p.5), em seu livro *The Onlife Manifesto: Being a Human in a Hyperconnected Era*, aponta que o surgimento de tecnologias comunicacionais permitiu a transformação do cenário atual do mesmo modo em que a escrita marcou a passagem da pré-história para a história. De acordo com ele, a atualidade pode ser percebida como hiper história, em que o limite entre o real e o virtual não existe e há um fluxo muito maior de informações e capacidade de processamento delas.

Nesse sentido, o autor identifica que houveram transformações na forma como o ser humano é entendido. Agora, as pessoas são entes informacionais que interagem constantemente com outros entes, sejam eles outras pessoas, dispositivos, máquinas ou a própria internet. Dessa maneira, a Figura 1 visa elucidar o conceito proposto por Floridi (2015, *apud* Souza, 2021), em que o ser informacional se encontra cercado de outros entes, dentre os quais fazem parte dispositivos conectados, pessoas e a própria internet.

Figura 1 - Seres informacionais



Fonte: De autoria própria

Em suma, esse cenário de hiperconectividade digital pode ser resumido como "a condição existencial repleta de conexões digitais, surgida com o acesso popularizado à rede mundial de computadores, cuja facilidade de comunicação e informação gera novos comportamentos e costumes" (LOPES, 2016, p.1).

Levando em consideração esse cenário de conectividade e transformações, os *smartwatches* podem ser entendidos como dispositivos que contribuem para essa realidade, uma vez que possuem capacidade computacional de se conectar com outros dispositivos, coletar dados pessoais e fornecer notificações (CECCHINATO et al., 2015).

Por causa dessa característica informacional — de coleta, compartilhamento de dados e envio de notificações —, esses dispositivos levantam diversas questões éticas em relação à segurança e privacidade dos usuários. Alguns exemplos dessas questões podem ser percebidos como a relação entre a conveniência e a invasão de privacidade no envio de notificações (HANSON, 2023), assim como riscos à segurança dos dados como ataques, vulnerabilidade de acesso à informação e venda de dados para terceiros (PORITIU, 2024).

Diante disso, a presente pesquisa objetiva responder às seguintes questões:

- Os usuários estão informados em relação aos dados que são coletados ao seu respeito?

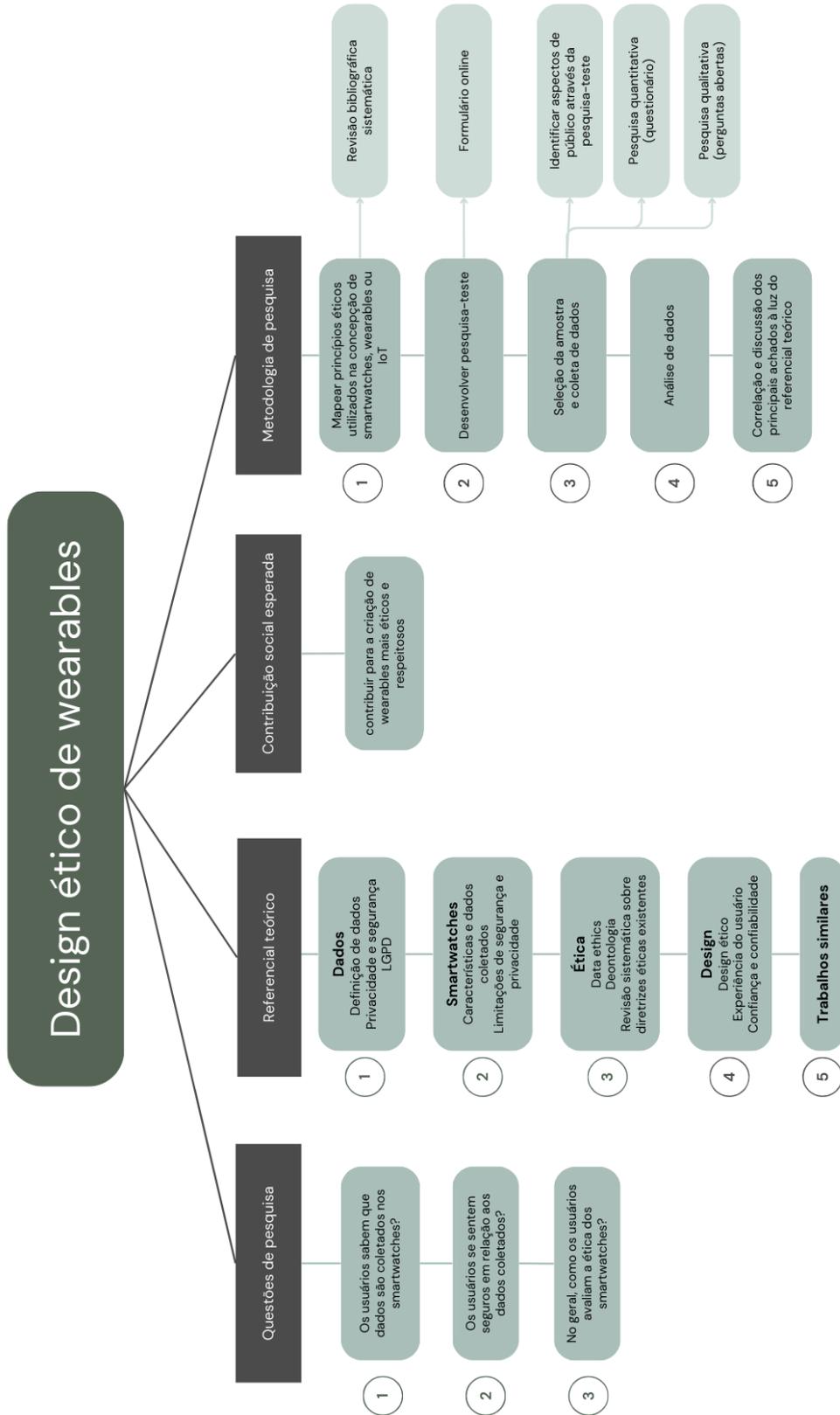
- Os usuários se sentem seguros em relação à privacidade e segurança de seus dados?
- E por fim, como essas questões éticas são percebidas e o quanto elas afetam suas experiências de uso?

Além disso, o estudo busca validar ou refutar as seguintes hipóteses:

- a maioria dos usuários não têm total visibilidade e ciência sobre os dados coletados a seu respeito;
- a falta de transparência sobre o uso de dados faz com que a maioria dos usuários não se sintam seguros;
- tal desconhecimento preocupa em parte os usuários, uma vez que a sensação de insegurança e falta de privacidade se tornam um "mal necessário" para a interação com o dispositivo, não gerando impacto negativo o suficiente para afastar o usuário do artefato.

Visando explorar e descobrir todas essas questões, a pesquisa apresentará a seguinte configuração, conforme apresentado no mapa mental representado na Figura 2.

Figura 2 - Mapa conceitual da pesquisa (autoria nossa)



Fonte: De autoria própria

1.3 OBJETO DE ESTUDO

Levando em consideração a contextualização e as questões éticas abordadas anteriormente, o objeto de estudo da presente pesquisa são as percepções dos usuários acerca da ética, segurança e privacidade dos *smartwatches*. Através da coleta dessas impressões, pretende-se contribuir para o design e desenvolvimento de wearables mais éticos.

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Mapear o conhecimento, a confiança e as experiências dos usuários em relação aos dados coletados por smartwatches, a fim de não apenas compreender o estado atual de consciência e percepção sobre segurança e privacidade, mas também transformar essas informações em insumos que orientem práticas de design e desenvolvimento responsáveis. Dessa forma, as percepções dos usuários servem como guia para que designers e desenvolvedores possam mitigar fragilidades identificadas e antecipar riscos éticos no uso desses dispositivos.

1.4.2 Objetivos Específicos

Sendo assim, os objetivos específicos deste trabalho são:

- realizar uma revisão da literatura sobre as diretrizes e desafios éticos associadas ao uso de *smartwatches*;
- desenvolver e validar um instrumento de pesquisa para medir o nível de confiança e ciência dos usuários de *smartwatches*;
- coletar dados por meio de uma pesquisa quantitativa junto a uma amostra representativa de usuários;
- analisar os dados coletados para identificar os principais fatores que influenciam a confiança deles e suas preocupações éticas relacionadas ao uso desses dispositivos;
- e por fim, investigar o impacto das preocupações éticas na experiência de uso dos smartwatches, visando à formulação de diretrizes éticas para designers e desenvolvedores.

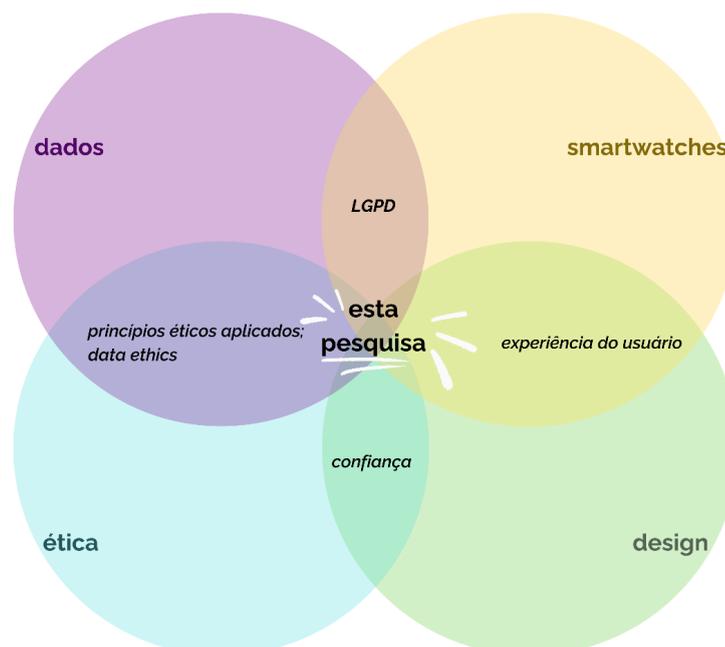
2. REFERENCIAL TEÓRICO

Tendo em vista compreender mais sobre a temática a ser investigada, a saber mapear a experiência dos usuários de smartwatches, o presente capítulo será detalhado em quatro tópicos que servirão de base teórica para fundamentar o estudo:

- inicialmente, tratar de temas elementares como o conceito de dados pessoais, bem como sobre a LGPD e suas limitações em garantir a segurança e privacidade dos usuários;
- sobre *smartwatches*, conceituação, principais funcionalidades apresentadas e questões éticas a eles associadas;
- ética, suas definições, qual sua importância na concepção dos artefatos conectados, bem como uma revisão sistemática das diretrizes éticas existentes relacionadas aos *smartwatches* e *wearables* em geral;
- sobre o design, como ele se relaciona com a ética e *smartwatches*, estabelecendo uma experiência para os usuários e uma relação de confiança.

Dessa forma, esses quatro tópicos compõem a conceituação da pesquisa da seguinte forma, conforme mostra a Figura 3.

Figura 3 - Tópicos a serem discutidos a seguir



Fonte: De autoria própria

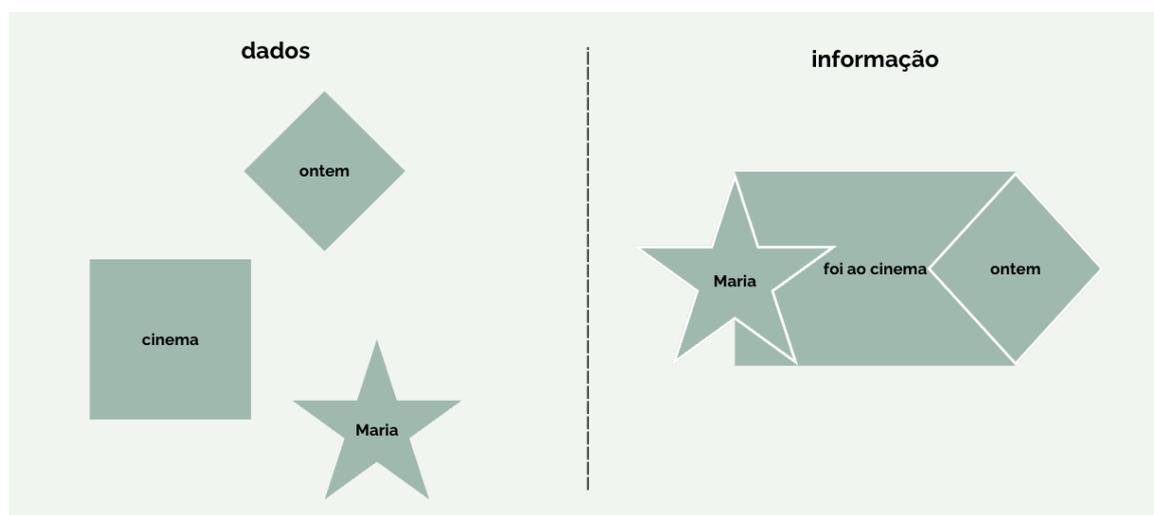
2.1 DADOS

Para iniciar as discussões, o conceito mais elementar a respeito do tema proposto diz respeito à definição de dados e de dados pessoais. Essas informações iniciais servirão de base para a discussão sobre a importância da privacidade e segurança de usuários de *smartwatches*.

2.1.1 Dados - Definição geral

De acordo com Janeček (2018), dados correspondem a fatos. São conteúdos desconexos coletados através de sensores e outras tecnologias como aplicativos e formulários online. Ao contrário do termo informação, o dado não possui significado a menos que seja unido a outros dados e, dessa forma, seja passível de interpretação se tornando assim, uma informação. Sendo assim, dados e informações, embora utilizados como sinônimos, possuem diferentes significados. A Figura 4, a seguir, ilustra esses conceitos.

Figura 4 - Exemplo da diferença entre dados e informação



Fonte: De autoria própria

Os dados ainda podem ser classificados como pessoais e não pessoais. Segundo o Tribunal de Justiça Eleitoral (TRE, 2020), a LGPD categoriza como dados pessoais as informações que permitem a identificação de uma pessoa direta ou indiretamente. Exemplos de dados pessoais seriam nome, CPF, data de nascimento, endereço IP, localização, fotos, entre outros. Dentro dessa classificação

ainda, existem os chamados dados pessoais sensíveis, que, segundo a LGPD, incluem a dados sobre:

"...origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dado referente à saúde** ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;" (*Autoridade Nacional de Proteção de Dados, 2024*, grifo nosso)

Neste estudo, serão analisados os dados pessoais relacionados à saúde dos usuários, coletados nos *smartwatches*. A LGPD proíbe o uso ou compartilhamento desses dados para fins lucrativos, permitindo exceções apenas em casos necessários para a prestação de serviços de saúde, assistência farmacêutica ou diagnósticos e tratamentos em benefício do paciente, titular das informações (Brasil, 2018, Art. 11, II, "a").

Dessa maneira, embora fabricantes de *smartwatches* possam coletar dados de saúde dos usuários para otimizar a experiência e fornecer serviços, é importante destacar que a comercialização ou o compartilhamento desses dados, visando lucro é vedada pela legislação, caso possam identificar o usuário. A questão da privacidade, portanto, emerge como uma preocupação central para os consumidores, especialmente quando se lida com tecnologias que acessam informações tão sensíveis.

O próximo tópico abordará como a privacidade é tratada no contexto da proteção de dados e quais são os desafios enfrentados pelos usuários e empresas na era digital.

2.1.2 Privacidade e segurança

Henrique (2024) relata que as primeiras discussões publicadas sobre privacidade tiveram seu início em 1890, no artigo "*The right of privacy*" de Warren e Brandeis. Nele, foi definido que a privacidade correspondia ao "direito de ficar sozinho" ou "de ser deixado em paz". No contexto atual, de hiperconectividade, onde as informações pessoais circulam por toda parte, o conceito de privacidade permaneceria o mesmo?

Segundo Henrique (2024), não. Embora a privacidade continue sendo um direito fundamental humano, conforme prevêem os Direitos Humanos, atualmente ela

se limita ao uso e compartilhamento de informações pessoais ou sensíveis para fins indevidos. Isso porque, devido à quantidade de dispositivos, aplicativos e outras tecnologias que captam informações a todo momento, a fim de gerar com esses dados lucro, é praticamente impossível uma pessoa ter total privacidade. Conforme Correia de Jesus (*apud*, Henrique 2024, p.13) afirma:

"De uma forma geral, empresas e estados querem conhecer os seus consumidores e cidadãos, respectivamente, monitorizar comportamentos e prever atuações futuras, seja para fins comerciais ou de segurança. As informações pessoais são hoje valiosos activos para as empresas, que recolhem cada vez mais dados em prol da sua eficiência e rentabilidade, elaborando posteriormente completíssimos perfis de consumo".

Sendo assim, a privacidade, especialmente no contexto digital, tornou-se uma questão que vai além do controle individual dos usuários. Na verdade, Nissenbaum afirma que o que preocupa os usuários não é a restrição do fluxo de informações—ou seja impedir que as informações sejam compartilhadas—, mas a **garantia de que esse fluxo de dados flua adequadamente** (*apud*, Sui et al.,2023).

Por isso, embora as pessoas possam adotar práticas para proteger seus dados, como configurar senhas seguras e limitar o compartilhamento de informações, a verdadeira responsabilidade sobre esse fluxo de dados recai sobre as regulamentações, as empresas que coletam e processam esses dados e, principalmente, sobre *designers* e desenvolvedores enquanto *gatekeepers* (porteiros) (Papanek, 1971), ou como responsáveis pelas inovações disponibilizadas para a sociedade.

Como poderá ser visto a seguir, leis como a LGPD foram criadas para proteger os direitos dos indivíduos, mas sua eficácia depende da aplicação rigorosa por parte das autoridades e do comprometimento das organizações em implementar práticas robustas de segurança e transparência. Nesse cenário, a privacidade se torna um bem que precisa ser garantido não apenas pelo usuário, mas, principalmente, por quem detém o poder e os recursos para protegê-la.

2.1.3 LGPD e suas limitações

A LGPD, assim como a GDPR da União Europeia, é responsável por determinar que práticas acerca da coleta, compartilhamento e processamento de dados podem ser adotadas pelas empresas e órgãos controladores.

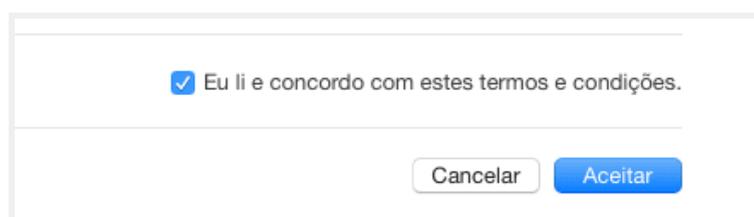
A respeito da garantia à privacidade e segurança do usuário e das suas informações pessoais, a LGPD, no art. 5º, inciso XI, incentiva o uso de técnicas de anonimização das informações, para impedir que os dados coletados consigam identificar a pessoa usuária. O art. 46 determina ainda que as empresas responsáveis pela coleta de dados devem se utilizar de técnicas administrativas para proteger esses dados sensíveis e impedir o acesso indevido, bem como o vazamento para o público (Brasil, 2018).

Conforme analisa Henrique (2024), a lei, embora sendo importante para garantir a segurança do usuário, não consegue amparar completamente o usuário nessa questão. Muitas lacunas ainda são deixadas, abrindo espaço para que as empresas cumpram a regulamentação da forma como lhes aprouver.

Nesse sentido, ele aponta o consentimento como a principal fraqueza da regulamentação. Embora a lei determine que o usuário deva consentir explicitamente com a coleta, processamento e compartilhamento de seus dados, ela não determina de que forma esse consentimento precisa ser realizado.

Dessa forma, as empresas o fazem com um simples clique a um termo de política de privacidade –conforme a Figura 5–, que devido à extensão e complexidade de entendimento, o usuário não lê e muitas vezes aceita para ter acesso a aplicativos gratuitos, conteúdos online ou acessar determinados serviços em aplicativos ou dispositivos (Carvalho, 2024 p.17).

Figura 5 - Aceite dos termos e condições



A imagem mostra uma interface de usuário para a aceitação de termos e condições. No topo, há uma barra de busca vazia. Abaixo, há um campo de texto com o texto "Eu li e concordo com estes termos e condições." precedido por uma caixa de seleção marcada com um ícone de checkmark azul. Na base da caixa, há dois botões: "Cancelar" (botão desativado) e "Aceitar" (botão ativo em azul).

Fonte: CESAR, 2018

Nesse sentido, Sui et al. (2023) apontam que esse consentimento rápido, sem a leitura completa ou total compreensão das políticas de privacidade, pode levar as empresas a extraírem mais informações além das necessárias, o que pode causar danos ao usuário. Sobre isso, os autores afirmam:

“Isso pode levar a práticas de coleta de dados avisos de que, se comunicados de outra forma claramente, muitos usuários provavelmente não aceitariam. Na verdade, esta prática esmagadora é extremamente eficaz, com um estudo estimando que 97% das pessoas indicam concordância com uma política de privacidade que deve levar aproximadamente 30 minutos para ler, em apenas 51s. A exclusão dessas políticas de coleta de dados é problemática, já que a mera operação de alguns wearables de consumo se baseia na transferência livre e “consensual” de todos os dados do dispositivo para a empresa. A extensa agregação de dados pelas empresas atende a vários propósitos. Primeiro, os dados podem ser usados para analisar a demonstração gráficos da base de usuários de wearables para identificar quem são os consumidores do produto e que tipo de comportamento(s) eles realizam, que por extensão, podem ser vendidos para análises e empresas de marketing. Dessa forma, as empresas de wearables atuam como ‘corretores de dados’, adquirindo, fundindo, analisando e compartilhando dados pessoais com ‘incontáveis destinatários’. Segundo, dados podem ser usados para ensinar IA. Mais especificamente, conjuntos de dados de ‘proporções sem precedentes’ são usadas para treinar algoritmos como prever, influenciar e adaptar melhor ao consumidor”. (tradução nossa)

Além desse consentimento sem leitura dos termos, dispositivos conectados como a IoT contribuem para agravar esse cenário de extração de dados e dificuldade em controlar quem pode ter acesso ou não, conforme aponta Carvalho (2024). Isso porque, embora esses dispositivos colem conteúdos desconexos, quando unidos, revelam muito mais informações sobre os usuários do que se imagina.

Por isso, entender mais sobre esses dispositivos ajuda a compreender melhor o quanto a ética e principalmente, a ética profissional de designers e desenvolvedores, pode contribuir para a segurança e privacidade do usuário.

2.2 SMARTWATCHES

A respeito do *smartwatch*, um conceito importante para o entendimento do dispositivo e preocupações éticas a seu respeito é a definição de IoT, classe de dispositivos da qual os smartwatches fazem parte.

Devido à propriedade de conexão entre si, com outros dispositivos e interação com humanos, uma IoT possui a capacidade de modificar a forma como as pessoas interagem com as coisas (Tzafestas S. G., 2018).

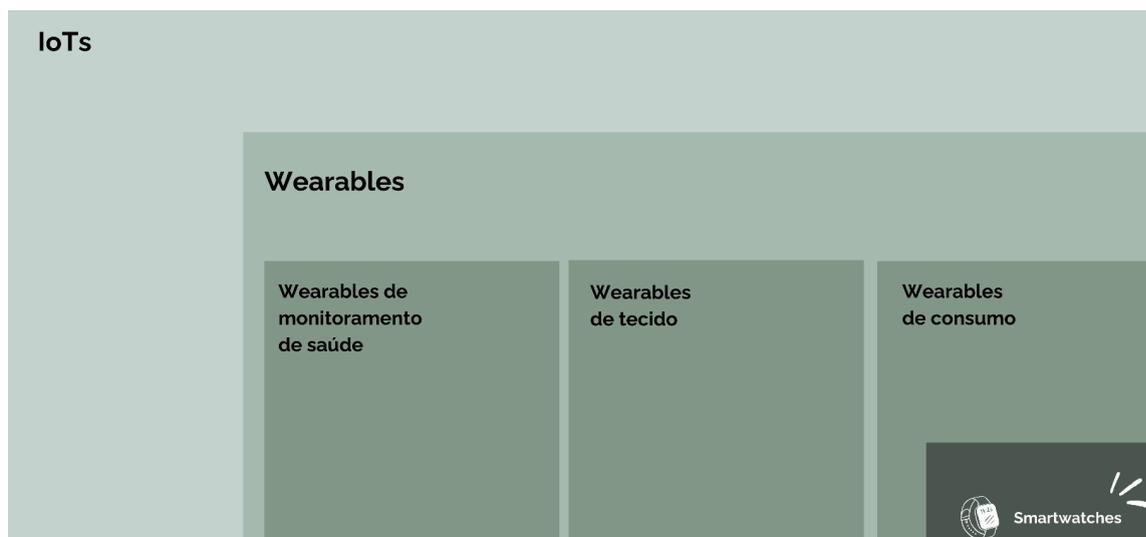
Por causa disso, esses dispositivos são importantes, pois elevam a capacidade da internet para além da conexão com dispositivos já utilizados anteriormente como celulares e computadores, incluindo novos aparelhos. Com isso, esses dispositivos formam um ecossistema de fluxo de dados e permitem que as pessoas desfrutem de mais serviços e facilidades (Sorri; Mustafee; Seppänen, 2022).

Dentro da IoT, fazem parte os dispositivos chamados de *wearables* ou vestíveis que, como o próprio nome sugere, são os aparelhos inteligentes utilizados no corpo como acessórios. Exemplos de vestíveis são tecidos, relógios, óculos, anéis, entre outros que possuem sensores. Esses dispositivos podem ser classificados da seguinte forma (Allhoff; Henschke, 2018):

- de monitoramento de saúde;
- de tecido, tecidos inteligentes;
- de consumo como *smart tvs*, *smartwatches*, entre outros.

Em resumo, pode-se entender que os *smartwatches* são classificados, conforme a Figura 6 ilustra:

Figura 6 - Classificação dos smartwatches



Fonte: De autoria própria

Dada sua classificação como *wearables* de consumo, os *smartwatches* se destacam como dispositivos importantes no ecossistema IoT, por oferecer aos usuários uma gama de funcionalidades projetadas para facilitar a integração entre o digital e o físico. Essas funcionalidades vão desde o monitoramento de saúde até a sincronização com outros dispositivos inteligentes.

Ao longo dos anos, os smartwatches passaram por diversas transformações, ganhando mais e mais funcionalidades à medida que a tecnologia avançou. O primeiro *smartwatch*, por exemplo, o IBM Linux Watch, lançado nos anos 2000 (Cecchinato et al., 2015), foi projetado para exercer comunicação sem fio com computadores, celulares e outros dispositivos. Ele continha funcionalidades ainda presentes nos relógios atuais como a possibilidade de ler e-mails, receber mensagens, calendário, acessar endereços e lista de tarefas (IBM, 2001).

Atualmente, de acordo com Hajibabaei e Naik (2023), os *smartwatches* possuem diversos sensores como acelerômetro, barômetro e geolocalização, que permitem que eles desempenhem diversas funcionalidades com precisão. Dentre as funcionalidades mais comuns encontradas nesses dispositivos, pode-se encontrar:

Quadro 1 - Lista de funcionalidades comuns entre os smartwatches

Funcionalidades (Hajibabaei e Naik, 2023)
Monitoramento de passos
Monitoramento de atividade físicas, sabendo inclusive sugerir qual atividade o usuário está realizando
Monitoramento dos batimentos cardíacos
Uso de mapas
Rastreamento de dispositivos aos quais ele está conectado
Realização e recebimento de chamadas
Recebimento de notificações
Controle de gestos
Comando de voz
Controle de música
Realização de pagamentos
Detecção de queda
Realização de chamadas emergenciais

Conforme visto no Quadro 1, pode-se identificar que muitas das funcionalidades apresentadas coletam informações pessoais dos usuários, como é o caso da localização utilizada tanto no monitoramento de passos, como no monitoramento de atividades físicas. Tais informações demandam uma preocupação maior com a segurança do usuário.

Sendo assim, autores como Fawle e Leblanc (2024) defendem que a segurança dos dispositivos deve ser construída nos estágios iniciais de desenvolvimento do produto, pois as funcionalidades presentes no smartwatch, embora facilitem a vida dos usuários, possibilitam a exposição a vulnerabilidades em relação à segurança de dados pessoais e privacidade dos usuários (Hajibabaei e Naik, 2023). O Quadro 2, a seguir, contém uma lista de vulnerabilidades mapeadas nos smartwatches.

Quadro 2 - Vulnerabilidades de segurança e privacidade encontradas nos *smartwatches*

Vulnerabilidades de segurança e privacidade	Descrição	Autores			
		Wang (2017)	Karakaya et al. (2016)	Beg et al. (2023)	Fawle; Leblanc (2024)
Autenticação	Os <i>smartwatches</i> utilizam pouca ou nenhuma autenticação, confirmações de perfil.	X	X	X	
Criptografia	Não há o uso de criptografia nos dados coletados para dificultar o roubo e interpretação das informações.	X	X	X	
Interface	Interfaces inseguras que facilitam a troca de senhas em contas utilizadas no relógio.		X		
Contas	Nem todos os aplicativos utilizados nos <i>smartwatches</i> exigem do usuário a criação de senhas fortes, nem protegem os dados por eles coletados da forma devida. Esses fatores podem facilitar o vazamento de dados pessoais.		X		
Conexão	Os <i>smartwatches</i> se conectam via bluetooth a outros dispositivos. Tal meio oferece riscos de segurança, uma vez que não possui autenticação e permite que o dispositivo seja sempre encontrável e possível de conexão.			X	X
Software/Firmware	Embora firmwares maldosos, quando identificados, não são possíveis de serem instalados nos <i>smartwatches</i> , eles são baixados e analisados dentro do sistema, o que pode comprometer a segurança do usuário.		X		

Conforme visto no Quadro 2, os smartwatches possuem diversas vulnerabilidades que podem facilitar o roubo e vazamento de informações pessoais importantes como dados vitais e de rastreamento, o que pode causar diversos impactos sociais negativos aos usuários. Principalmente, porque, como afirma Beg et al. (2023), "dados uma vez divulgados, estão disponíveis para sempre".

De acordo com a empresa de soluções financeiras Naskar (2024), os smartwatches levantam três grandes preocupações em relação à segurança e à privacidade de dados. A primeira diz respeito ao monitoramento contínuo: por coletar informações do usuário a todo instante, o dispositivo pode causar a sensação de vigilância constante e insegurança, já que o indivíduo não conhece a real extensão das informações coletadas. A segunda refere-se ao compartilhamento de dados com terceiros, visto que muitos dispositivos repassam informações a empresas parceiras para análise de perfil e direcionamento de publicidade. Por fim, destaca-se a retenção dos dados, relacionada à forma como são armazenados e ao período de armazenamento, que frequentemente se tornam alvos de ataques.

Essas vulnerabilidades ampliam os riscos, já que novas formas de ataques digitais são continuamente desenvolvidas, como é o caso de roubo de dados através de sinais ultrassônicos (Cybersecurity Brazil, 2025). Entre elas, podem-se citar: a possibilidade de hackers acessarem informações pessoais e financeiras para revendê-las em mercados clandestinos ou aplicarem golpes, como o roubo de identidade; a ameaça à segurança física do usuário por meio do uso da localização e de seus hábitos de movimento; além da utilização desses dados para o direcionamento de publicidades indesejadas, baseadas em seu perfil de consumo, estilo de vida ou necessidades de saúde (Cote et al., 2023).

Por isso, é importante que *designers* e desenvolvedores pensem na forma como a tecnologia influencia a vida das pessoas, seus hábitos e comportamentos, bem como nos riscos de privacidade e segurança das informações (Roossien, C. C. et al., 2021)

Para concluir as vertentes necessárias para esse estudo, é necessário ainda identificar fatores como a ética e a confiança são importantes para a experiência do usuário.

2.3 ÉTICA: CONTEXTUALIZAÇÃO E CONCEITOS

Ao discutir a evolução da ética, A. Schweitzer (1958, p. 69) destaca uma distinção entre o ponto de vista do homem primário em relação ao do homem moderno. Segundo ele, o homem primário tendia a limitar suas responsabilidades éticas aos membros de sua tribo ou comunidade imediata, uma mentalidade que reflete uma compreensão restrita do que constitui o seu círculo de preocupação ética.

No entanto, à medida que a sociedade avança em direção à modernidade, surge uma consciência expandida das interconexões sociais e da responsabilidade moral. O compromisso ético se estende não apenas aos familiares e vizinhos, mas também à sociedade como um todo e à humanidade em geral. Nessa visão mais contemporânea, a noção de fraternidade universal se destaca.

Dentro desse contexto de civilização e modernidade, as primeiras sociedades modernas desenvolveram o conceito de ética de acordo com as suas necessidades. Nesse sentido, tem-se a Grécia Antiga como referência ocidental pioneira na discussão ética e difusão desse conhecimento.

Em seu sentido original, a palavra ética vem do grego *ethos*, que significa costumes ou hábitos, e é compreendida ainda como a ciência que avalia as ações e o caráter humano, visando diferenciar as virtudes (os acertos) dos vícios (os erros) (Tayung, 2019). Sendo assim, a ética é a área do conhecimento que visa compreender que ações são consideradas corretas e que critérios são utilizados para definir como acertada (Lopes, 2018).

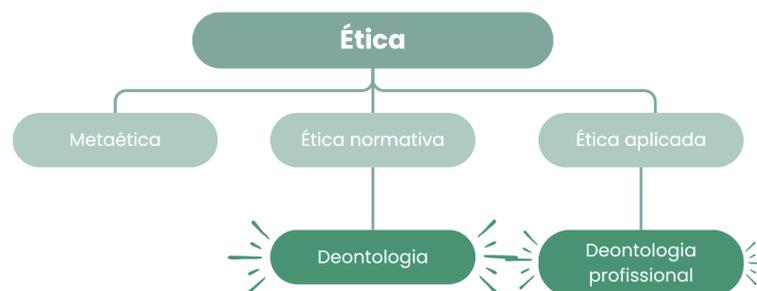
Ao longo do tempo, conforme a filosofia foi se desenvolvendo como campo de conhecimento, o senso de ética foi evoluindo e, dentro do campo filosófico, a ética atualmente se divide em metaética, ética normativa e ética aplicada. Da metaética fazem parte investigações que têm como objetivo refletir sobre o que é a moral, de que forma ela pode ser alcançada.

Já da ética normativa, fazem parte as normas que regulamentam as ações humanas. Por último, a ética aplicada é composta pela racionalização e comportamentos que visam tornar as outras formas de ética, que são teóricas, em

prática. Essa última abrange as tomadas de decisões tanto em relação à vida cotidiana, como também em relação à concepção de produtos e serviços (A. Adam, 2008).

Dentro dessas vertentes, esse estudo abordará o que há de mais recente na ética normativa, com foco na linha deontológica, bem como na ética aplicada, com foco na deontologia profissional, visto que essas áreas melhor correspondem ao objetivo do projeto. A Figura 7 ilustra os conceitos abordados.

Figura 7 - Esquema visual que ilustra o tema a ser tratado



Fonte: De autoria própria

2.3.1 Ética normativa e deontológica

De acordo com Lopes (2018), a ética normativa corresponde à investigação sobre os padrões de comportamento considerados certo e errado, com o objetivo de definir como as pessoas devem pensar e se comportar. Dessa forma, surgem normas éticas que regulamentam a sociedade.

A ética normativa possui duas vertentes: a teleológica e a deontológica. Resumidamente, a ética teleológica determina quais ações são corretas de acordo com o objetivo que se pretende alcançar, enquanto a ética deontológica determina que ações são éticas de acordo com as normas estabelecidas, independentemente do objetivo a ser alcançado ou das consequências que cause.

Devido ao seu caráter normativo e universalista, a ética deontológica faz mais sentido para esse trabalho, uma vez que é relacionada ao conjunto de normas universais que conseguem determinar boas práticas (Santos e Serafim, 2023).

De acordo com Stanford Encyclopedia of Philosophy, a palavra deontologia vem do grego *deon* (dever) e *logia* (estudo) e refere-se a "ao domínio das teorias morais que orientam e avaliam nossas escolhas do que devemos fazer (teorias deônticas), em contraste com aquelas que orientam e avaliam que tipo de pessoa somos e devemos ser" (Alexander; Moore, 2024).

Dentro da deontologia, existem diversas teorias que partem do mesmo princípio de investigar a ética sob a perspectiva da norma, ao invés do resultado. Fazem parte da deontologia a ética do discurso, do dever, contratualista e institucionalista.

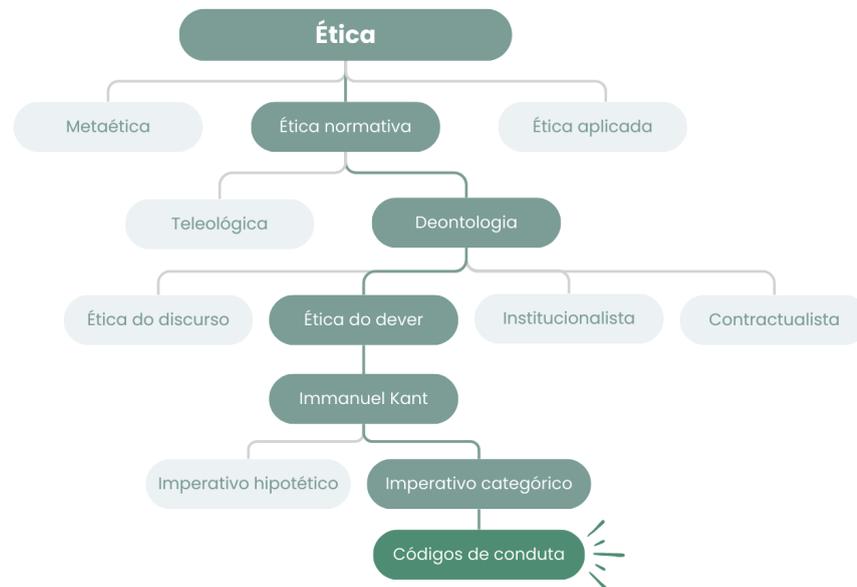
Dessas, no entanto, se destaca a ética do dever, de Immanuel Kant, cuja premissa é a de que a ética deve ser centrada no dever. Nesse sentido, o dever "gera uma obrigação, forçando-o a fazer o que talvez não quisesse ou que pelo menos não o agradaria porque o homem é imperfeito e carrega em si sentimentos contraditórios" (Lopes, 2018).

Diz-se que a ética, dentro desse pensamento, deve discriminar o certo do errado através do que é chamado de imperativo. Na visão de Kant, existem dois tipos de imperativos: o hipotético e o categórico. Enquanto o hipotético tenta determinar como deve ser a ação para chegar a determinado fim, o categórico norteia as ações de acordo com a reflexão se aquela ação poderia ser considerada uma lei universal de comportamento, sem sofrer alterações.

Seguindo o viés do imperativo categórico é que surgem os códigos de conduta, que nada mais são do que um conjunto de regras com o objetivo de uniformizar e universalizar formas corretas de agir. Um exemplo conhecido de códigos de ética é o estabelecido e juramentado pelos médicos. Todos os profissionais, independentemente da área médica exercida, precisam juramentar as mesmas normas de conduta, sob a punição de, ao descumprir, perder o direito de exercer a profissão e ainda sofrer punições governamentais (Alexander; Moore, 2024).

Dessa forma, os conceitos apresentados nesse tópico podem ser ordenados da seguinte forma, conforme pode ser visto na Figura 8:

Figura 8 - Esquema visual a respeito de todos os conceitos descritos neste capítulo



Fonte: De autoria própria

Em se tratando do desenvolvimento de produtos de dados, o funcionamento difere do proposto por Kant. Geralmente, a tecnologia é concebida e utilizada antes da definição de códigos de conduta, o que abre espaço para usos antiéticos, ilegais ou que possam causar danos ao usuário (Ibiricu; Van Der Made, 2020). A ausência de diretrizes relacionadas ao desenvolvimento de produtos tecnológicos dificulta a responsabilização adequada em casos de prejuízos. Ainda assim, o tema tem ganhado destaque em debates acadêmicos e institucionais, evidenciando a urgência de estabelecer normas que mitiguem riscos e assegurem os direitos dos usuários.

2.3.2 Data ethics e a ética profissional do designer

A ética aplicada tem sido amplamente discutida com o objetivo de nortear as ações humanas no que diz respeito à concepção de produtos tecnológicos e à utilização de informações pessoais. Nesse cenário, destacam-se os conceitos de ética informacional e data ethics, propostos por Luciano Floridi, que se distanciam da ética clássica ao abordarem a conduta humana no atual contexto de fluxo massivo de dados.

Segundo o autor, a filosofia informacional é o campo que investiga os princípios fundamentais da informação, bem como sua aplicação em diversas áreas.

Ele compara a sociedade informacional a uma árvore cujas folhas crescem de forma acelerada e desordenada, enquanto suas raízes éticas não acompanham esse crescimento (Floridi, 2010 *apud* Gonzalez de Gomez, 2024). Em sua visão, há mais moralidade nos setores governamentais, institucionais e empresariais do que na vida cotidiana de milhões de indivíduos.

Floridi argumenta que a sociedade contemporânea é composta por entes informacionais que trocam dados continuamente. Dessa forma, a ética deixa de ser centrada em princípios universais — como propõe a ética clássica — e passa a ser centrada no ente impactado. Como afirma o autor: “essa abordagem da ética coloca o receptor da ação, o paciente, no centro do discurso ético, e desloca seu remetente, o agente, para sua periferia” (Floridi, 2010 *apud* Gonzalez de Gomez, 2024, p. 728).

Essa perspectiva indica que, no contexto da hiperconexão, a ética deve colocar o usuário — aquele que sofre os impactos dos dispositivos lançados no mercado — no centro das discussões. Já os designers, desenvolvedores e demais envolvidos no processo de criação devem ocupar a posição de escuta, atentos às necessidades, vulnerabilidades e expectativas desses usuários.

Com base nesse entendimento, essa abordagem faz sentido para aplicação neste trabalho, uma vez que objetiva considerar a experiência dos usuários como elemento central para a formulação de diretrizes éticas aplicadas ao desenvolvimento de tecnologias.

Floridi também observa que os dispositivos digitais modernos são artefatos autônomos, informados e capazes de executar ações moralmente relevantes de forma independente, podendo causar tanto “bem artificial” quanto “mal artificial”. Por isso, “o discurso ético deve incluir a análise de seu design, implantação, controle e comportamento, como parte de uma estratégia maior para entender uma série de novas questões éticas, não apenas em Informação e Informática” (Floridi, 2010 *apud* Gonzalez de Gomez, 2024).

Além disso, o conceito de data ethics introduz a necessidade de considerar a ética em todas as etapas do ciclo de vida dos dados — desde a coleta até o processamento e compartilhamento das informações dos usuários. De forma

complementar, os profissionais envolvidos no desenvolvimento de produtos tecnológicos também precisam se pautar por códigos de ética que legitimem suas práticas e os obriguem a considerar, com responsabilidade, a segurança e a privacidade dos usuários.

2.3.3 Ética profissional aplicada ao design

Entre as vertentes da ética aplicada, destaca-se a criação de códigos de conduta, compreendidos como um conjunto de diretrizes normativas que definem condutas consideradas apropriadas em uma empresa, instituição ou profissão. Seu principal objetivo é orientar ações baseadas em princípios positivos a serem seguidos por todos os membros da comunidade.

Considerando que a ética diz respeito às ações humanas dentro de contextos específicos, a ética profissional pode se apresentar sob duas formas: uma mais ampla, relacionada às práticas que uma organização espera de seus colaboradores independentemente da função que exerçam; e outra, mais específica, voltada à conduta esperada de profissionais de uma mesma área de atuação.

De modo geral, essas condutas esperadas compõem os chamados códigos de conduta — documentos criados para promover harmonia e coerência no trabalho das equipes, baseando-se em valores como justiça, integridade e responsabilidade (Trevino; Nelson, 2021). Por isso, profissões como a Medicina exigem um compromisso ético formal, simbolizado pelo juramento profissional, cuja validade transcende o local de atuação. Ainda que o código de ética não assegure condutas sempre corretas, ele possibilita responsabilização e sanções em caso de descumprimento (Monteiro, 2019).

No entanto, ao contrário dessas profissões regulamentadas, o campo do design — especialmente o design de produtos digitais — ainda carece de códigos de conduta amplamente reconhecidos e adotados (How [...], 2015). Dessa forma, decisões éticas no design acabam ficando a critério dos valores e interpretações individuais dos profissionais, o que pode resultar em práticas que comprometem a experiência e até a segurança dos usuários (Monteiro, 2019).

Assim, a ética profissional no design é essencial para garantir que os produtos e serviços desenvolvidos gerem impactos positivos na vida das pessoas.

No caso dos designers de wearables, como smartwatches, esse compromisso ético vai além da estética e da usabilidade: envolve a responsabilidade de proteger dados sensíveis dos usuários, especialmente informações relacionadas à saúde e ao bem-estar. Nessa perspectiva, o conceito de *data ethics* torna-se central.

Para apoiar essas práticas, diretrizes específicas de segurança e privacidade são indispensáveis. Nesse contexto, o tópico a seguir trata de revisão de literatura que busca mapear as diretrizes éticas existentes e identificar lacunas, contribuindo para a construção de uma atuação profissional mais responsável e alinhada às necessidades do cenário digital contemporâneo.

2.4 DIRETRIZES ÉTICAS E ESTRATÉGIAS DE SEGURANÇA E PRIVACIDADE DOS USUÁRIOS DE WEARABLES

A respeito da ética relacionada aos wearables em geral, alguns autores identificaram possíveis direcionamentos e estratégias para melhorar e garantir a segurança desses dispositivos. Para analisar tais publicações, foi necessário realizar uma revisão de literatura. Nesse sentido, o presente capítulo trata-se da tradução e reprodução da metodologia, bases e termos de busca, bem como os resultados e conclusão presentes no artigo “*Ethical Guidelines Related to Wearable Devices: a literature review*”, (Oliveira; Teixeira, 2025), de autoria própria.

2.4.1 Estratégia de Busca e Seleção de Fontes

A busca nas fontes foi realizada em bases de dados acadêmicas relevantes, incluindo IEEE Xplore, ScienceDirect, PubMed e Google Acadêmico. O uso do Google Acadêmico visou complementar a estratégia de busca expandindo a cobertura, especialmente em relação à literatura cinzenta ou artigos relevantes que podem não ser indexados em bases de dados mais restritivas.

Embora o Google Acadêmico não seja uma base de dados científica tradicional, estudos metodológicos anteriores por exemplo, Gusenbauer e Haddaway (2020) e Haddaway et al. (2015) reconhecem seu valor em revisões sistemáticas quando utilizado com critérios de inclusão transparentes e rigorosos — como os aplicados nesta revisão.

O período incluiu artigos publicados entre 2014 e 2024, período marcado pelo desenvolvimento significativo de dispositivos vestíveis e pelo discurso intensificado sobre privacidade e segurança de dados. Para identificar materiais relacionados a este estudo, as seguintes palavras-chave foram usados em inglês e português:

- *wearables* or dispositivos vestíveis
- *ethical guidelines* or diretrizes éticas
- *data privacy* or privacidade de dados
- *data security* or proteção de dados
- *limitations* or limitações
- *challenges* or desafios

2.4.1.1 Combinações de termos de pesquisa

As pesquisas foram realizadas usando a seguinte combinação de palavras-chave (strings de pesquisa):

- Combinação 1: (*wearables* OR “dispositivos vestíveis”) AND (“*ethical guidelines*” OR “diretrizes éticas”) AND (“*data security*” OR “proteção de dados”) AND (*challenges* OR “desafios”)
- Combination 2: (*wearables* OR “dispositivos vestíveis”) AND (“*ethical guidelines*” OR “diretrizes éticas”) AND (“*data privacy*” OR “privacidade de dados” OR “*data security*” OR “proteção de dados”) AND (*limitations* OR “limitações” OR *challenges* OR “desafios”)
- Combination 3: (*wearables* OR “dispositivos vestíveis”) AND (“*data privacy*” OR “privacidade de dados”) AND (“*ethical guidelines*” OR “diretrizes éticas”)
- Combination 4: (*wearables* OR “dispositivos vestíveis”) AND (“*ethical guidelines*” OR “diretrizes éticas”) AND (“*data privacy*” OR “privacidade de dados” OR “*data security*” OR “proteção de dados”)

2.4.1.2 Processo de Seleção e Filtragem

As publicações encontradas foram selecionadas através das seguintes etapas:

1. Leitura do título

2. Remoção de artigos duplicados e de acesso restrito
3. Leitura do resumo
4. Leitura do texto completo

É importante esclarecer que a triagem por título foi utilizada como uma etapa inicial de exclusão para gerenciar um grande volume de resultados de forma eficiente e eliminar estudos claramente não relacionados. Essa abordagem é comum e justificada em revisões sistemáticas e integrativas, particularmente em áreas exploratórias ou onde a variação terminológica é alta, como em estudos interdisciplinares envolvendo tecnologia e ética.

A decisão de selecionar inicialmente por título não compromete a confiabilidade da revisão, pois resumos e textos completos foram revisados nas etapas seguintes para determinar a elegibilidade para inclusão. Esse processo de filtragem em várias etapas permite um equilíbrio entre abrangência e viabilidade no gerenciamento de grandes conjuntos de dados durante a síntese da literatura.

- Critérios de Inclusão: Artigos em inglês ou português que abordassem diretrizes ou regulamentações éticas com foco em privacidade e segurança de dispositivos vestíveis foram considerados. Foi dada preferência a estudos e publicações revisados por pares de fontes confiáveis.
- Critérios de Exclusão: Estudos cujo título não se enquadrava no tema a ser estudado, nos quais não havia termos relacionados às buscas, como "ética", "Internet das Coisas" e "segurança e privacidade". Além disso, estudos cujo resumo e outros conteúdos focavam exclusivamente em aspectos técnicos, sem qualquer conexão com diretrizes éticas ou que não abordassem privacidade e segurança também foram eliminados.

2.4.2 Validação e Garantia de Confiabilidade

Os processos de seleção e triagem foram conduzidos criteriosamente, como revisão por pares, seguindo critérios de inclusão e exclusão predefinidos. Para aumentar a confiabilidade da revisão, as decisões de triagem foram discutidas entre os autores sempre que necessário, especialmente em casos de incerteza quanto à

elegibilidade dos artigos. Essa abordagem colaborativa garantiu maior consistência na aplicação dos critérios e contribuiu para o rigor metodológico da revisão.

2.4.3 Análise de Dados

Após a seleção, as publicações foram analisadas de forma descritiva e exploratória, com o objetivo de organizar as diretrizes em categorias temáticas amplas, como princípios gerais e tecnologias específicas de proteção de dados. Devido à diversidade de abordagens e formatos das diretrizes identificadas, optou-se por uma análise qualitativa, sem aplicar critérios rigorosos de comparação entre as diretrizes, dada a variabilidade de perspectivas encontradas. As informações foram sintetizadas com foco na descrição de conceitos e diretrizes relevantes, além da identificação dos principais desafios éticos abordados na literatura.

2.4.4 Limitações Metodológicas

Embora a revisão tenha seguido uma estratégia estruturada de busca e seleção de fontes, trata-se de uma revisão narrativa da literatura, e não sistemática. Portanto, algumas limitações devem ser observadas:

- Revisão não exaustiva: A análise não incluiu critérios de avaliação da qualidade das fontes e teve como objetivo fornecer uma visão exploratória e panorâmica.
- Falta de padronização: A diversidade e a falta de consistência em algumas publicações limitaram a possibilidade de análise comparativa de padrões e lacunas entre as diretrizes.

2.4.5 Resultados

O Quadro 3 mostra as 16 publicações analisadas após o processo de leitura e escolha descrito no tópico Processo de Seleção e Filtragem.

Quadro 3 - Publicações analisadas na revisão

Referência	Título	Contexto de aplicação
Wang, Y. (2024)	The Design Dilemma of Personalized Health Applications: the Balance Between Meeting User Needs and Data Security	Saúde e segurança dos dados

Perez, A. J.; Zeadally, S. (2018)	Privacy Issues and Solutions for Consumer Wearables	Privacidade e wearables
Arias, O. et al. (2015)	Privacy and Security in Internet of Things and Wearable Devices	IoT e dispositivos vestíveis
Gaff, B. M.; Emerym, W. (2015)	Legal Issues with Wearable Technology	Legal
Lowens, B.; Motti, V. G.; Caine, K. (2017)	Wearable Privacy: Skeletons in the Data Closet	Saúde e informática médica
Mok, T. M.; Cornish, F.; Tarr, J. (2015)	Too Much Information: Visual Research Ethics in the Age of Wearable Cameras	Ética na pesquisa visual
Plogsties, E.; Professor, S.; Brino, V. (2023)	Balancing Wearables in the Workplace: Protecting Privacy and Human Rights-a Legal Analysis	Privacidade no trabalho
Qu, S.; Gao, X. (2020)	Analysis of Ethical Issues Involved in Wearable Equipment for Health Care	Saúde e ética
Roossien, C. C. et al. (2021)	Ethics in Design and Implementation of Technologies for Workplace Health Promotion	Saúde no local de trabalho
Seneviratne, S. et al. (2017)	A Survey of Wearable Devices and Challenges	Revisão de wearables
Sui, A. et al. (2023)	Ethical considerations for the use of consumer wearables in health research	Pesquisa em saúde
Van Der Linden, D. et al. (2019)	Buddy's Wearable Is Not Your Buddy: Privacy Implications of Pet Wearables	Dispositivos para pets
Marengo, L. L. et al. (2022)	Mobile technologies in healthcare: reflections on development, application, legal aspects, and ethics	Saúde e aspectos legais
Nature Medicine (2022)	Walking the tightrope between data sharing and data protection	Compartilhamento de dados
Yang, C. et al. (2019)	An Empirical Study on the Data Security and Privacy Awareness to Use Health Care Wearable Devices	Saúde e consciência sobre privacidade
Yang, M.; Guo, J.; Bai, L. (2020)	A Data Privacy-preserving Method for Students' Physical Health Monitoring by Using Smart Wearable Devices	Monitoramento de saúde escolar

Com base na diversidade dos materiais revisados, diretrizes éticas para o uso de wearables foram identificadas em diversos contextos de aplicação, incluindo monitoramento da saúde humana, coleta de dados de animais de estimação, coleta

geral de dados e áreas especializadas, como processamento de dados genômicos. Consequentemente, as estratégias para garantir segurança e privacidade variam dependendo do contexto da aplicação, refletindo diferentes desafios éticos e operacionais.

Entre as soluções mais comuns citadas estão a autenticação e a criptografia para proteger dados sensíveis (Yang, Guo e Bai, 2020; Seneviratne et al., 2017; Gaff e Emery, 2015; Nature Medicine, 2022; Wang, 2024; Perez e Zeadally, 2018; Lowens, Motti e Caine, 2017; Mok, Cornish e Tarr, 2015; Plogsties, Professor e Brino, 2023). No entanto, embora medidas técnicas como a criptografia sejam amplamente recomendadas, vários autores (Lowens, Motti e Caine, 2017; Mok, Cornish e Tarr, 2015; Wang, 2014) enfatizam que confiar apenas em proteções técnicas pode ser eticamente insuficiente, pois não garantem o consentimento informado ou o empoderamento do usuário. Essa divergência sugere uma lacuna crítica entre a viabilidade técnica e a responsabilidade ética nas abordagens atuais.

Alguns estudos, notadamente Mok, Cornish e Tarr (2015), defendem uma estratégia de privacidade desde o design, propondo práticas de desenvolvimento centradas no usuário. No entanto, relativamente poucos estudos discutem como operacionalizar de forma prática a participação do usuário no processo de design, indicando uma limitação na profundidade das estratégias de implementação.

A importância da minimização de dados é reconhecida por Marengo et al. (2022) e Roossien et al. (2021), alinhando-se a padrões internacionais como o GDPR. No entanto, há pouco consenso entre as fontes analisadas sobre como equilibrar a minimização de dados com as demandas funcionais das tecnologias vestíveis, especialmente em aplicações de saúde e bem-estar, onde dados extensos são frequentemente coletados para fins preditivos.

Responsabilidade e transparência são destacadas por Lowens, Motti e Caine (2017), sugerindo que as empresas não devem apenas implementar tecnologias de proteção, mas também adotar práticas de comunicação responsáveis com os usuários. No entanto, uma avaliação crítica dos estudos revela a falta de propostas detalhadas para mecanismos de fiscalização regulatória ou de verificação de conformidade.

Por fim, embora Arias et al. (2015) e Roossien et al. (2021) defendam a necessidade de regulamentações mais rigorosas, os estudos revisados raramente abordam como as disparidades regulatórias globais (como entre o GDPR na Europa e leis menos rigorosas em outros lugares) podem impactar a implantação ética de wearables internacionalmente.

Assim, embora a literatura revisada identifique princípios fundamentais para orientar práticas éticas em tecnologias vestíveis, ainda existem desafios significativos na tradução desses princípios em ações consistentes, executáveis e sensíveis ao contexto. Isso destaca a necessidade de pesquisas futuras que preencham a lacuna entre a teoria ética e a aplicação prática.

2.4.6 Discussão

Com base na revisão bibliográfica realizada, fica evidente que as preocupações com a segurança e a privacidade dos usuários de dispositivos vestíveis se intensificaram na última década, como refletido no crescente número de publicações acadêmicas sobre o assunto. No entanto, apesar da expansão das discussões, ainda não existe uma abordagem universal ou padronizada para garantir a proteção do usuário, em grande parte devido à diversidade de contextos de aplicação e à natureza fragmentada das estratégias propostas.

Os resultados sugerem que, embora a aplicação de princípios éticos gerais — como transparência, responsabilização e minimização de dados — forneça uma base importante, sua implementação prática permanece inconsistente em diferentes domínios. Além disso, soluções técnicas como criptografia leve e criptografia autenticação multifatorial é amplamente recomendada, mas por si só é insuficiente para proteger totalmente os usuários sem medidas complementares que promovam o consentimento informado e o design centrado no usuário.

Assim, garantir o uso ético de tecnologias vestíveis requer não apenas a combinação de estratégias técnicas e éticas, mas também uma abordagem mais sensível ao contexto que leve em conta os riscos específicos associados a cada aplicação. Além disso, a análise crítica revela uma necessidade urgente de desenvolvimento de marcos regulatórios mais robustos e executáveis que preencham a lacuna entre as diretrizes éticas e as práticas do mundo real.

Pesquisas e políticas futuras devem priorizar a operacionalização de princípios éticos de maneiras adaptáveis, transparentes e executáveis na prática em diversos contextos globais.

2.5 DESIGN: ÉTICA E EXPERIÊNCIA DO USUÁRIO

“O bom design é HONESTO.” Essa é a sexta das dez máximas de Dieter Rams sobre o bom design. Nesse princípio, o autor destaca que o produto não deve parecer mais inovador ou tecnológico do que realmente é, evitando manipular o usuário por meio de falsas impressões (Teixeira, 2012).

Assim como Rams defende a honestidade no design, autores como Don Norman (2004) ampliam a discussão ao destacar que o impacto emocional e a experiência de uso são determinantes para a forma como o usuário percebe a integridade de um artefato. A experiência, portanto, não se limita ao desempenho funcional, mas também envolve respostas afetivas que reforçam — ou enfraquecem — a confiança depositada no produto. Sendo assim, se a honestidade é exigida do produto como parte da experiência do usuário, a fim de construir uma relação de confiança, **o que se pode dizer sobre o designer que o projeta?**

As discussões sobre a responsabilidade ética no design remontam a Victor Papanek (1971), um dos pioneiros a se preocupar com essa temática. Em seu livro *Design for the Real World: Human Ecology and Social Change*, ele compara os designers a porteiros (gatekeepers), profissionais que atuam como mediadores entre o que é idealizado e o que é lançado no mercado. Assim, possuem uma responsabilidade moral e social com a sociedade e o meio ambiente por cada produto que permite “passar” do conceito à realidade de consumo. Além disso, Papanek afirmava que os designers têm o dever de criar artefatos que sejam benéficos ao mundo, atendendo às necessidades reais das pessoas, especialmente daquelas em condições mais precárias (Monteiro, 2017).

Com o tempo, e à medida que os produtos se tornaram mais complexos e intangíveis, essas discussões tornaram-se ainda mais necessárias e frequentes (Zillig, 2019). Nessa perspectiva, o design ético pode ser compreendido de forma mais ampla como a criação de empresas, produtos e serviços fundamentados em

princípios de justiça e respeito para com todos os envolvidos (Falbe, Andersen e Frederiksen, 2020, tradução nossa).

Por outro lado, quando se trata da aplicação prática desses princípios éticos no desenvolvimento de interfaces, produtos ou serviços, ainda não há diretrizes universais ou amplamente aceitas sobre o que é ou não ético. Isso ocorre porque, diferentemente da pesquisa científica, o desenvolvimento de produtos envolve um cenário mais complexo e variável, o que dificulta a formulação de regras que abarquem todos os contextos e projetos (Nielsen, 2021).

Ainda assim, autores como Mike Monteiro (2017), designer e palestrante sobre ética, têm se dedicado à reflexão e à construção de diretrizes práticas para o exercício ético da profissão. Segundo ele, os designers possuem quatro grandes responsabilidades ao tomarem decisões em seus projetos:

- **Com o mundo:** para Monteiro, o design é, por definição, uma atividade voltada à solução de problemas em benefício da sociedade. Por isso, os designers devem escolher com critério quais problemas resolver, priorizando, por exemplo, as necessidades de minorias sociais em vez de atender aos interesses de grupos privilegiados.
- **Com o ofício:** cada projeto influencia a forma como o design é percebido e como outros profissionais trabalham. Um projeto antiético compromete a reputação do campo como um todo, exigindo que outros designers se esforcem para reconstruir a confiança do público.
- **Com os clientes:** é dever do designer alertar o cliente sobre possíveis implicações éticas de um projeto, recusar-se a executar propostas que considere prejudiciais e orientar o cliente quanto a soluções mais responsáveis.
- **Consigo mesmo:** cada projeto assinado por um designer carrega seus valores e constrói sua imagem profissional. Assim, a responsabilidade consigo envolve refletir sobre o legado que se deseja deixar e como se quer ser reconhecido na profissão.

Dessa forma, a ética no design de artefatos não se restringe a criar produtos que gerem impactos positivos para o mundo e para as pessoas. Ela também está

relacionada à maneira como o design é compreendido enquanto prática e à imagem que seus profissionais constroem a partir das escolhas que fazem.

Sendo assim, a ética na criação de artefatos implica não só em soluções que causam bons impactos para o mundo e as pessoas, mas também em uma melhor percepção sobre o design em si e seus especialistas. Um dos aspectos centrais dessa percepção é a construção da confiança entre usuário e produto.

De acordo com Desmet (2012, apud Santos, 2018), a confiança é uma das 25 emoções positivas experienciadas pelos usuários na relação com o produto com o qual interagem. Nesse sentido, o ato de confiar corresponde à abdicação do controle por parte de quem confia, escolhendo apenas gerenciar suas expectativas sobre o outro. Para Hardin (2002), só se escolhe confiar em algo ou alguém porque essa coisa ou pessoa demonstrou ser digna de confiança. Esse julgamento ocorre, segundo o autor, com base em dois fatores principais: (1) o outro possui um compromisso moral com a confiança depositada; e (2) tem caráter para ser digno dela.

Essa relação entre confiança e emoção pode ser aprofundada a partir da perspectiva de Norman (2004), que explica como o design atua em três níveis: visceral (reação imediata à aparência), comportamental (usabilidade e desempenho) e reflexivo (significados e valores). A confiança nos artefatos digitais depende, portanto, não apenas da funcionalidade técnica, mas também da capacidade de engajar emocionalmente o usuário nesses diferentes níveis.

No campo do design de produtos digitais, como os *wearables*, esse raciocínio se mostra ainda mais sensível. A confiança do usuário é constantemente solicitada, uma vez que, como afirma Luhman (1979, apud Eloffson, 2001), a confiança começa onde o conhecimento se limita. Diante de tecnologias vestíveis, o usuário não possui plena visibilidade sobre os processos de coleta, armazenamento e compartilhamento de dados. Assim, ele precisa confiar não apenas no artefato em si, mas também nos profissionais e empresas por trás do produto.

De acordo com Paul et al. (2024), a confiança em produtos e empresas está ligada à capacidade dessas entidades de cumprir seus deveres de forma positiva e responsável. Quando o usuário tem uma experiência satisfatória com um produto,

essa confiança tende a se fortalecer. Yang et al. (2019), por exemplo, observaram que usuários que vivenciam boas experiências com wearables tendem a se preocupar menos com a segurança do dispositivo — evidenciando a correlação entre confiança e experiência de uso.

Dessa forma, pode-se compreender que o desenvolvimento ético e respeitoso de produtos digitais — como os dispositivos vestíveis — é fundamental não só do ponto de vista moral, mas também estratégico. A confiança do usuário se torna um indicador de sucesso do produto, pois está diretamente associada à qualidade da experiência que ele proporciona.

Como defende Norman (2013), o design centrado no usuário é essencial para que a interação seja fluida e transparente, fortalecendo a confiança. Nesse sentido, mapear percepções e emoções durante o processo de uso não apenas amplia a satisfação, mas também sustenta uma relação de credibilidade entre usuários, designers e empresas.

Consequentemente, quanto mais os designers se empenharem em envolver o usuário desde o início do processo de concepção, adotando princípios éticos e técnicas de proteção de dados, maior será a **transparência percebida**, e mais sólida será a **confiança estabelecida**. Isso implica um compromisso do design com a segurança, a privacidade e a clareza no fluxo de informações, fortalecendo a credibilidade do produto e da marca. Mapear como está a experiência do usuário — bem como suas percepções e preocupações éticas — torna-se, portanto, uma etapa essencial para melhorar continuamente o processo de design de artefatos digitais.

3. METODOLOGIA

De acordo com a definição de Gerhardt e Silveira (2009, p.5), o presente estudo se configura como pesquisa quantitativa, uma vez que visa investigar a opinião dos usuários sobre a ética dos *smartwatches* de forma geral. Partindo desse pressuposto, a pesquisa se divide em etapas nas quais os dados são coletados, tratados e analisados de forma sequencial.

A primeira etapa consiste na revisão da literatura que pode ser encontrada no tópico 2.4 e no artigo de título “*Ethical Guidelines Related to Wearables: Literature Review*” nos quais foram identificadas publicações acerca dos princípios e diretrizes éticas referente ao desenvolvimento dos *wearables*, especificamente em relação à segurança e privacidade dos dados. Além disso, foram mapeados os desafios e impactos presentes no cenário atual, conforme listado no tópico 2.2.1.

A segunda etapa consiste no desenvolvimento do instrumento de coleta de dados. Tal fase consiste na elaboração de um questionário estruturado que contemple indagações relacionadas aos objetivos e hipóteses da pesquisa. Esse instrumento de coleta deve ser validado por meio de pré-teste com usuários em que, a depender dos resultados obtidos, pode haver refinamentos nas questões elaboradas.

Após essa etapa, a próxima corresponde à seleção da amostra e coleta de dados. Fazem parte dessa fase as atividades de definir os critérios de inclusão para seleção da amostra, considerando aspectos como idade, gênero, frequência de uso de *smartwatches* e uso de diferentes modelos, visando identificar possíveis vieses na pesquisa. Também está incluída a atividade de realizar a coleta de dados por meio de perguntas estruturadas, utilizando os questionários online elaborados na fase anterior.

Após validado o questionário piloto e realizados os devidos ajustes, caso necessário, a quarta etapa corresponde a uma nova disponibilização do formulário, dessa vez abrangendo uma amostra maior e mais diversa de participantes.

Sendo assim, a quinta etapa corresponde à análise de dados. Dentro dessa fase, serão utilizadas técnicas estatísticas adequadas para analisar os dados

quantitativos coletados, como análise descritiva e análise exploratória para identificar padrões e relações entre variáveis.

A sexta etapa consiste na integração dos resultados em que serão correlacionadas as respostas para obter uma compreensão abrangente das hipóteses levantadas no estudo e objetivos da pesquisa.

Por fim, na última etapa, serão discutidos os resultados à luz da literatura revisada e das teorias relevantes, destacando contribuições para o conhecimento acadêmico e prático. Também serão apresentadas conclusões sobre o nível de confiança dos usuários e preocupações éticas identificadas.

4. ELABORAÇÃO DO QUESTIONÁRIO E PESQUISA DE TESTE

Conforme descrito no capítulo anterior, o presente capítulo trata da segunda e terceira etapas da pesquisa, que correspondem à descrição do processo de elaboração do questionário, bem como a definição dos critérios de inclusão e exclusão dos participantes, aplicação da pesquisa de teste e os ajustes realizados após a análise dos resultados preliminares.

4.1 ELABORAÇÃO DO QUESTIONÁRIO

Para o desenvolvimento do questionário, foram necessários definir qual o perfil de público, quais as perguntas a serem feitas, bem como a forma como elas seriam respondidas pelos participantes. Para nortear essas decisões, foi necessária a pesquisa e leitura de artigos e dissertações que utilizaram técnicas de coleta de dados similares e que dessa forma pudessem contribuir para a pesquisa.

Sendo assim, dentre os artigos pesquisados, utilizou-se 3 trabalhos similares como referência, conforme será apresentado adiante. De acordo com o Quadro 4, de cada trabalho diferentes aspectos foram utilizados como referência, a saber:

Quadro 4 - Pesquisas similares e suas contribuições

Referência	Contribuições
Choudhury; Shamszare (2023)	<ul style="list-style-type: none"> • Elaboração de pesquisa-teste preliminar utilizando uma escala Likert, abrangendo desde "concordo fortemente" até "discordo fortemente"; • Cada item do questionário foi elaborado com base nas hipóteses iniciais dos autores; • Aplicou-se uma fórmula estatística específica para validar a pesquisa-teste, assegurando a confiabilidade e a validade dos resultados obtidos; • A validação estatística é de suma importância para garantir a robustez dos dados coletados e a consistência das conclusões derivadas do estudo.
Furnell, Jusor e Katsabas (2006)	<ul style="list-style-type: none"> • Desta referência foram identificadas questões demográficas que visam mapear o perfil dos participantes. Incluem perguntas como gênero, faixa etária, grau de escolaridade, frequência de uso do dispositivo; • Avaliou-se o grau de consciência dos respondentes sobre as funcionalidades de segurança; • Cuidou-se para evitar qualquer viés nas respostas dos participantes, garantindo a imparcialidade e a integridade dos dados coletados;
Koohang et al. (2021)	<ul style="list-style-type: none"> • Deste estudo foram identificadas a metodologia de elaboração das questões em escala Likert de acordo com os objetivos e hipóteses a serem validadas no estudo.

Com base nessas referências e contribuições, foram elaboradas as perguntas listadas no Quadro 5. No quadro, ainda, é possível perceber que cada pergunta foi elaborada tendo em vista responder a uma questão de pesquisa e/ou hipótese levantada no início deste estudo, cumprindo assim o objetivo do estudo.

Quadro 5 - Relação entre as questões de pesquisa e hipóteses e perguntas elaboradas para o questionário

Questão de Pesquisa / Hipótese	Pergunta aplicada no questionário
<p>Questão de pesquisa: O quão informados os usuários estão em relação aos dados que são coletados a seu respeito?</p> <p>Hipótese: Os usuários não têm total visibilidade e ciência sobre os dados coletados a seu respeito.</p>	<ul style="list-style-type: none"> • Você poderia citar alguns dados que o seu relógio coleta a seu respeito? <p>Essa é uma questão aberta em que os usuários precisaram escrever o que sabem.</p> <ul style="list-style-type: none"> • Tenho conhecimento total sobre quais dados são coletados a meu respeito <p>Essa questão está formatada em escala Likert de 1 a 5, sendo 1 discordo totalmente e 5 concordo totalmente.</p>
<p>Questão de pesquisa: O quão seguros os usuários se sentem em relação à privacidade e segurança de seus dados?</p> <p>Hipótese: A falta de transparência sobre o uso de dados faz com que os usuários não se sintam seguros;</p>	<p>Permanecendo no formato de escala Likert de 1 a 5, as seguintes perguntas visam identificar como os usuários percebem a segurança e privacidade dos dispositivos</p> <ul style="list-style-type: none"> • sempre sou informado sobre os dados que estão sendo utilizados; • utilizando o meu próprio smartwatch sei onde posso cancelar o fornecimento dos meus dados pessoais; • me sinto vigiado pelo meu smartwatch; • me sinto completamente seguro utilizando esse dispositivo; • sinto que meus dados pessoais estão seguros e protegidos; • me sinto incomodado quando meu smartwatch compartilha dados com outros dispositivos meus, como celular e computador, sem o meu consentimento ou ciência.

<p>Questão de pesquisa: Como essas questões éticas são percebidas e o quanto elas afetam suas experiências de uso?</p> <p>Hipótese: Tal desconhecimento preocupa em parte os usuários, mais especificamente nos momentos iniciais de interação com o dispositivo. No entanto, conforme o utilizam, a ética deixa de ser uma preocupação ao mesmo tempo em que a sensação de insegurança e falta de privacidade se tornam um "mal necessário".</p>	<ul style="list-style-type: none"> ● sinto que não posso confiar totalmente no meu smartwatch; ● percebo que não consigo me sentir à vontade quando utilizo o meu smartwatch; ● deixo de realizar certas atividades quando estou utilizando o meu smartwatch.
---	--

Além das questões apresentadas acima, outras perguntas foram adicionadas com o objetivo de mapear características e comportamentos dos participantes, bem como identificar possíveis vieses. Essas perguntas foram elaboradas tendo em vista coletar informações relevantes, preservando a identidade e privacidade dos respondentes. Assim, perguntou-se aos pesquisados:

- Em qual região você mora?
- Com que gênero você mais se identifica?
- Qual a sua faixa etária?
- Qual o seu nível de escolaridade?
- Com que frequência você utiliza o seu *smartwatch*?
- Com que objetivo você geralmente utiliza o seu *smartwatch*?

Por fim, tendo elaborado todas as questões, criou-se o termo de consentimento. Esse será o primeiro item que os respondentes lerão, podendo discordar ou concordar com ele. Nele foram explicados os objetivos da pesquisa,

bem como expostas todas as informações que seriam coletadas a fim de trazer transparência e obter o consentimento informado dos participantes.

Uma vez que não foi objetivo da pesquisa coletar informações pessoais dos respondentes, como nome, email, telefone, o formulário se enquadra como pesquisa de opinião pública sem identificação dos participantes, o que, segundo as normas do Comitê de Ética da Universidade Federal de Pernambuco (UFPE), não necessita de submissão para avaliação (UFPE, 2016). Dessa forma, a estrutura final do questionário pode ser encontrada no Apêndice A.

4.2 RESULTADOS PARCIAIS

Como forma de divulgação do questionário, utilizou-se as redes sociais como Whatsapp, LinkedIn e Instagram, para que a maior diversidade de respondentes pudesse ser alcançada. Sendo assim, o questionário foi disponibilizado e divulgado durante 15 dias, alcançando assim um total de 28 respostas. Dentre essas, somente 26 foram consideradas respostas válidas, visto que 2 participantes alegaram não possuir *smartwatch* ou nunca ter usado um.

Sendo assim, entre os 26 participantes, 21 deles (80,8%) moram na região Nordeste, 2 no Sul, 2 no Sudeste e 1 no Centroeste. Dentre eles ainda, 16 (61,5%) se identificam com o gênero masculino, enquanto 10 (38,5%) se identificam com o feminino.

A respeito da faixa etária, 7 são jovens, tendo entre 18 a 24 anos, 12 são adultos entre 25 e 34 anos, 5 possuem entre 35 e 44 anos e apenas 2 possuem entre 45 e 54 anos. Por fim, a respeito da escolaridade, 18 deles (69,2%) possuem ensino superior completo, enquanto 5 ainda não o completaram; 2 completaram o ensino médio e 1 possui ensino fundamental completo.

Isso significa que a pesquisa de teste alcançou pouca diversidade demográfica, principalmente regional e educacional. Isso pode ser explicado pelo fato de essa pesquisa ter sido enviada para a rede de contatos próxima da pesquisadora, o que no nosso ponto de vista não compromete os resultados da pesquisa de teste em si, ainda que seja um ponto importante a ser levado em consideração.

Quando perguntados acerca da frequência de uso do dispositivo, 12 (46,2%) participantes afirmaram utilizar todos os dias. Outros 9 (34,6%) afirmaram que usam smartwatches quase todos os dias, apenas 4 responderam que utilizam o aparelho para realizar atividades específicas e 1 afirmou que raramente lembra de usar o dispositivo.

Quanto ao principal objetivo de uso, 10 participantes responderam que utilizam o smartwatch para obter mais facilidade e conexão. Outros 10 afirmaram que seu objetivo é monitorar atividades físicas específicas, 5 responderam monitorar a saúde e apenas 1 por moda e estilo. Nesse sentido, a pesquisa de teste teve uma melhor distribuição da amostra que em relação às características demográficas, alcançando diferentes frequências e objetivos de uso do dispositivo, o que demonstra que os usuários terão percepções distintas sobre a ética do aparelho.

Acerca dos dados coletados pelos *smartwatches*, os participantes demonstraram conhecimento diversificado, listando vários dados que têm ciência que o dispositivo coleta. As respostas mais frequentes em ordem decrescente foram: batimentos cardíacos, quantidade de passos, localização, qualidade do sono e oxigenação sanguínea. Outras respostas que apareceram com menos frequência foram: pressão arterial, ciclo menstrual, nível de estresse, quantidade de calorias gastas, entre outros.

Em se tratando das questões que visam testar a validade das hipóteses levantadas no início deste estudo e que possuem o formato de escala Likert, utilizou-se análise exploratória para realizar a interpretação dessas respostas (Análise [...], 2020). Para isso, precisou-se mapear o nível de concordância entre os respondentes, conforme a Figura 9, a seguir.

Figura 9 - Análise do nível de concordância entre os respondentes



A partir da análise desses resultados, pode-se observar que os usuários possuem um grau de concordância alto, afirmando que sim, se preocupam com a segurança das suas informações pessoais, mas ainda assim a maioria deles se sente seguro com o uso dos *smartwatches*, realizando atividades do dia a dia comumente, enquanto um número reduzido deles deixa de realizar certas atividades quando estão utilizando o dispositivo. Com isso, entende-se que as respostas obtidas com esse conjunto de perguntas, tendo uma abrangência maior de participantes, conseguiria testar a validade das hipóteses inicialmente levantadas.

Além dessas perguntas, a pesquisa ainda conta com um espaço aberto para que os respondentes possam compartilhar suas vivências com os *smartwatches*. Como não é um campo obrigatório do questionário, apenas 7 pessoas responderam. Dentre esses comentários, um participante escreveu que retira a localização e conexão *bluetooth* a fim de se sentir seguro. Outro escreveu se sentir profundamente vigiado e incomodado com o dispositivo. Outros dois, no entanto, afirmaram não se preocupar com suas informações pessoais, uma vez que já é frequente as notícias sobre vazamento de dados. Por fim, outros 3 ressaltaram sobre o quanto o dispositivo traz praticidade e ajuda em situações do dia a dia, principalmente no controle do estresse e ansiedade.

Por último, foi solicitado aos participantes que compartilhassem suas opiniões sobre a pesquisa. Apenas 1 respondeu que achou pouco objetiva. Os outros 25 pesquisados tiveram uma impressão positiva, afirmando achar que a pesquisa era curta, objetiva e levou pouco tempo para ser respondida.

4.3 CONCLUSÃO DO TESTE E MELHORIAS

Por meio dos resultados obtidos com a pesquisa de teste, pôde-se validar que as questões elaboradas conseguem testar as hipóteses levantadas no início do estudo, sem que isso demande muito tempo ou esforço cognitivo dos participantes.

Para aprimorar a análise dos dados, identificou-se a necessidade de coletar os endereços de e-mail dos participantes. Essa informação permitirá correlacionar as respostas dadas nas diferentes seções do questionário — como dados demográficos e percepções sobre segurança e confiança nos dispositivos —

possibilitando análises mais aprofundadas. Por exemplo, será possível verificar quantas pessoas da faixa etária de 18 a 24 anos demonstram confiar no dispositivo e na segurança de seus dados. No teste atual, essa triangulação não foi possível, pois a ausência do e-mail impediu o rastreamento das respostas individuais ao longo do questionário.

Além disso, notou-se a possibilidade de melhoria nas perguntas do questionário, adicionando perguntas sobre qual o nível de familiaridade do usuário com tecnologias em geral, bem como qual o modelo ou marca do dispositivo que ele utiliza. Também foi acrescentada a pergunta sobre o nível de preocupação dos usuários sobre a segurança e privacidade dos dados que ele tem ciência que o *smartwatch* compartilha. Essas informações darão melhor visibilidade sobre a experiência do usuário com o dispositivo.

Por fim, também houve a necessidade de estabelecer os critérios de inclusão e exclusão dos participantes. Na versão inicial, foram eliminados apenas os participantes abaixo de 18 anos ou que afirmaram não possuir o dispositivo. Na versão atual, além desses critérios, também foram eliminados os respondentes que:

- Raramente lembram de usar o dispositivo, visto que a baixa frequência de uso pode limitar a experiência do participante;
- Utilizam o dispositivo por moda ou estilo, já que tais usuários possivelmente utilizam menos as funcionalidades do dispositivo que coletam dados e por isso, não teriam a experiência afetada.

Após realizados os ajustes apontados acima, verificou-se que a nova versão do formulário precisaria ser submetida ao Comitê de Ética, devido à coleta do email dos participantes. Sendo assim, a pesquisa foi submetida e devidamente aprovada, conforme pode ser visto no Anexo A o parecer do Comitê. Nesse sentido, o Apêndice B mostra a nova versão do formulário após a aprovação do Comitê.

5. PESQUISA QUALITATIVA

Conforme proposto no tópico Metodologia, após a pesquisa de teste e os ajustes realizados, o formulário teve que ser disponibilizado novamente, desta vez para uma amostra maior de participantes.

Tendo em vista alcançar relevância estatística, a Universidade de São Paulo (2024) afirma que, quando a população é desconhecida, como é o caso do total de usuários de *smartwatches* no Brasil, pode-se utilizar uma proporção esperada de 0.5. Com isso, objetivando-se alcançar um nível de confiança de 95% com uma margem de erro de 5%, é possível calcular a quantidade de participantes (amostra) ideal para a pesquisa através da seguinte fórmula:

$$n = \frac{Z^2 \cdot p \cdot (1-p)}{e^2}$$

Onde:

- n: tamanho da amostra desejado;
- Z: valor correspondente ao nível de confiança (ex.: 1,96 para 95% de confiança);
- p: proporção esperada (se não houver uma estimativa, geralmente usa-se 50%, ou 0,5, que maximiza o tamanho da amostra);
- e: margem de erro desejada (ex.: 0,05 para 5%).

Com isso, para obter resultados expressivos, a pesquisa precisa alcançar um total de 385 participantes com respostas válidas, ou seja, 385 pessoas que possuem *smartwatch*, acima de 18 anos e que possuem o hábito de utilizar o dispositivo, por objetivos que não sejam moda ou estilo.

De forma semelhante à versão piloto, a pesquisa foi divulgada inicialmente em redes sociais como Whatsapp, LinkedIn e Instagram. Contudo, notou-se pouca diversidade regional nas respostas, como aconteceu durante o teste inicial.

Para mudar isso, foram enviados e-mails a todas as universidades federais e estaduais do Brasil, solicitando a divulgação da pesquisa, visto que a maioria dessas instituições possuem assessorias ou secretarias de comunicação que possuem acesso direto aos emails dos estudantes, professores e demais funcionários, o que

aumentaria a possibilidade de mais respostas serem obtidas, com maior diversidade de participantes.

Dessa forma, conseguiu-se obter, no período de 3 meses de divulgação, 665 respostas. Destas, todos os respondentes realizaram o consentimento em participar da pesquisa. Desses, 546 disseram ter maior idade e possuir um *smartwatch*, e com isso atenderam aos primeiros critérios de participação da pesquisa, avançando para as próximas perguntas.

Como decidir o consentimento e possuir um *smartwatch* eram as únicas questões obrigatórias, nem todos os participantes responderam o questionário todo. Contudo, a quantidade de respostas se mostra suficiente para análise e conclusão de resultados.

Para a análise dos resultados, foram utilizadas ferramentas estatísticas por meio da linguagem *Python* e da planilha Excel gerada a partir das respostas dos participantes. Inicialmente, os dados pessoais, como os endereços de e-mail, foram removidos a fim de preservar a privacidade dos respondentes. Essa exclusão também se justificou pelo fato de que a identificação individual não era relevante para os objetivos da pesquisa. O foco da análise concentrou-se em identificar padrões, correlações e tendências nas respostas, buscando compreender o comportamento geral dos participantes com base nos dados coletados.

A respeito das características demográficas dos participantes, a pesquisa conseguiu alcançar pessoas de quase todas as 5 regiões do Brasil, à exceção do Norte. Sendo assim, dentre os participantes a maior representatividade foi de nordestinos, somando-se 303 pessoas. A maioria das respostas são de pessoas que se identificam com o gênero masculino (300 ao todo; o gênero feminino ocupou um total de 240 respostas; 3 pessoas do gênero não-binário e 3 que preferiram não informar).

Os maiores percentuais de faixa etária foram dos 18 aos 24 anos (31,9%) e dos 25 aos 34 anos (31,3%), ou seja, a pesquisa conta em sua maioria com a percepção de jovens adultos. No entanto, ainda foi possível coletar percepções de faixas etárias mais velhas, como dos 45 aos 54 anos (11,5%), 55 aos 64 anos (2,7%) e mais que 64 anos (0,5%).

Em relação ao nível de escolaridade, a pesquisa atingiu em grande parte ao público já formado e de universitários (89,6%), o que já era esperado considerando que a pesquisa foi divulgada através das assessorias de comunicação das universidades do Brasil.

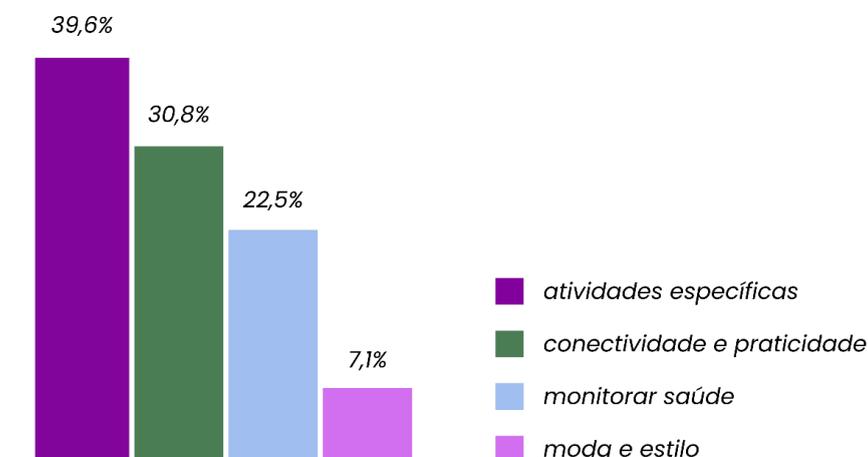
Ainda, a maioria dos respondentes apontou ter conhecimento avançado de tecnologia (67,6%), conseguindo aprender a utilizar sozinho e saber resolver problemas com os dispositivos com os quais interagem.

Quanto à frequência de uso, 57,5% apontaram utilizar todos os dias, enquanto 8,3% disseram raramente lembrar de usar. Esses últimos foram eliminados da pesquisa, visto que a frequência de uso é um critério importante para conseguir medir a experiência e relacionamento dos usuários com o dispositivo.

Em relação às marcas mais frequentes entre os participantes estão a Samsung (120 pessoas), em específico o modelo mais comum é o Galaxy Fit 3. Em seguida, os modelos mais comuns foram: o Apple Watch (93); Xiaomi (81); Amazfit (75).

Por fim, em relação às motivações de uso, as respostas demonstraram pouco mais de dispersão, tal como mostrado no Gráfico 1, 39,6% apontaram utilizar para monitorar atividades específicas; 30,8%, para ter mais conectividade e praticidade; 22,5%, para monitorar a saúde e 7,1%, por moda e estilo.

Gráfico 1 – Distribuição dos usuários por motivação de uso



Em resumo, a pesquisa corresponde às opiniões em sua maioria, de pessoas do gênero masculino, nordestinos, jovens adultos, formados ou universitários, que possuem conhecimento avançado em tecnologia e que utilizam seus smartwatches todos os dias, em geral para monitorar atividades específicas do seu dia.

Quando perguntados sobre quais os dados coletados os participantes tinham conhecimento que seu smartwatch coleta, 471 participantes se dedicaram a responder a essa questão. Dentre os resultados mais relevantes, estão os batimentos cardíacos, apontado por 390 pessoas; monitoramento do sono, incluindo tempo, profundidade e qualidade do descanso; quantidade de passos dados, calorias gastas, oxigenação e registro de exercícios físicos, seu tipo, tempo gasto e intensidade.

Além das respostas relacionadas a dados de saúde, os participantes também relataram, em menor quantidade, conhecer informações relacionadas à localização e uso do GPS, coleta de dados pessoais, como nome, idade e gênero; notificações e conexões com redes sociais.

Tais respostas demonstram que os usuários têm um conhecimento razoável acerca das informações coletadas, em relação à lista de funcionalidades apresentada no Quadro 1, no início da presente pesquisa. Embora todas as informações listadas apareçam nas respostas dos usuários, as maiores frequências se concentram em batimentos cardíacos, sono e quantidade de passos. Isso indica que suas respostas tendem a conter as informações que mais utilizam no seu cotidiano.

A análise apresentada no Gráfico 2 evidencia uma correlação significativa entre a faixa etária dos usuários e os objetivos de uso dos smartwatches. Observa-se que usuários mais jovens, especialmente entre 18 e 24 anos, tendem a utilizar os dispositivos com foco em praticidade, conectividade e estilo, refletindo um perfil mais tecnológico e estético. À medida que a idade avança, essa tendência se modifica: indivíduos das faixas de 25 a 44 anos demonstram maior preocupação com o monitoramento de atividades físicas e com a saúde.

Nas faixas etárias mais elevadas, especialmente entre 55 e 64 anos e acima de 64 anos, o uso dos smartwatches é quase exclusivamente direcionado ao

monitoramento da saúde, indicando uma mudança clara nas motivações conforme o envelhecimento da população.

Do ponto de vista estatístico, essa distribuição percentual entre idade e tipo de uso sugere a existência de uma associação significativa entre as variáveis. Visualmente, se verifica uma correlação positiva entre o aumento da idade e o uso voltado à saúde, enquanto o uso motivado por estilo ou conectividade tende a diminuir nas faixas etárias superiores. Esses resultados reforçam a importância de considerar o perfil etário no desenvolvimento e comunicação de tecnologias vestíveis, especialmente no que diz respeito à funcionalidade e ao propósito de uso.

Gráfico 2 - Distribuição da motivação de uso por faixa etária

Faixa etária	Motivação de uso			
	Moda e estilo	Monitorar a saúde	Monitorar atividades físicas	Ter mais praticidade
18 a 24 anos	10,3	15,5	34,5	39,7
25 a 34 anos	3,5	21,1	47,4	28,1
35 a 44 anos	2,5	32,5	40,0	25,0
45 a 54 anos	19,0	14,3	33,3	33,3
55 a 64 anos	0,0	60,0	40,0	0,0
mais que 64 anos	0,0	100,0	0,0	0,0

Para realizar uma análise sobre a segurança do usuário, buscou-se avaliar se os indivíduos que utilizam smartwatches com maior frequência no dia a dia possuem maior ou menor conhecimento sobre segurança e privacidade desses dispositivos. No Gráfico 3 observa-se que os participantes que demonstram menor preocupação com esses aspectos (100% deles) possuem, predominantemente, escolaridade correspondente ao ensino fundamental completo ou ensino médio incompleto.

Por outro lado, aqueles que atribuíram notas mais altas de preocupação (alta preocupação e preocupação em demasia) possuem, em sua maioria, ensino superior completo, o que sugere uma possível relação entre maior nível de escolaridade e maior conscientização sobre os riscos à segurança e privacidade associados ao uso desses dispositivos.

Gráfico 3 - Relação entre escolaridade vs nível de preocupação

Nível de preocupação com segurança e privacidade dos dados coletados pelo smartwatch

		Sem preocupação	Pouca preocupação	Preocupação moderada	Alta preocupação	Preocupação em demasia
Nível de escolaridade	Ensino Fundamental Completo	100,0	0,0	0,0	0,0	0,0
	Ensino Médio Completo	37,5	6,2	43,8	0,0	12,5
	Ensino Médio Incompleto	100,0	0,0	0,0	0,0	0,0
	Ensino Superior Completo	27,0	24,0	22,0	14,0	13,0
	Ensino Superior Incompleto	38,8	20,4	26,5	4,1	10,2

Outra correlação importante a ser analisada é se aqueles que mais utilizam o smartwatch no dia a dia demonstram alguma preocupação com a segurança e privacidade das informações geradas por esses dispositivos. O Gráfico 4 revela uma relação bastante curiosa: embora usuários que utilizam o smartwatch quase todos os dias ou todos os dias representem a maior parte dos respondentes, a proporção de indivíduos com alta preocupação e preocupação em demasia entre eles é relativamente baixa. Por exemplo, entre os que usam o dispositivo todos os dias, apenas 13,5% atribuíram nota máxima de preocupação, enquanto 32,7% demonstraram nenhuma preocupação.

Além disso, chama atenção que 66,7% dos usuários que utilizam o smartwatch apenas uma vez por semana atribuíram baixa preocupação mesmo entre os que usam menos. Esses dados sugerem que a frequência de uso não está diretamente associada a um maior cuidado com segurança e privacidade, contrariando a expectativa de que usuários mais habituais estariam mais conscientes sobre os riscos envolvidos.

Gráfico 4 - Relação entre frequência de uso vs nível de preocupação

Nível de preocupação com segurança e privacidade dos dados coletados pelo smartwatch

		Sem preocupação	Pouca preocupação	Preocupação moderada	Alta preocupação	Preocupação em demasia
Frequência de uso	1 vez por semana	0,0	66,7	0,0	33,3	0,0
	Para realizar atividades específicas	38,9	11,1	33,3	5,6	11,1
	Quase todos os dias	31,7	34,1	22,0	2,4	9,8
	Todos os dias	32,7	16,3	25,0	12,5	13,5

6. CONCLUSÃO

Esta pesquisa teve como objetivo investigar como questões éticas relacionadas à segurança e privacidade são percebidas pelos usuários de smartwatches, especialmente no que se refere à consciência sobre os dados coletados, ao sensação de segurança e à forma como essas percepções afetam sua experiência de uso. Com base nas perguntas de pesquisa e nas hipóteses formuladas, buscou-se compreender a experiência desses usuários a partir de um questionário aplicado a uma amostra significativa.

Os resultados obtidos permitiram confirmar, em parte, as hipóteses inicialmente propostas. Em relação à **visibilidade dos dados coletados**, observou-se que a maioria dos participantes possui um conhecimento razoável sobre as principais funcionalidades de seus dispositivos, especialmente aquelas relacionadas à saúde, como batimentos cardíacos, monitoramento do sono e contagem de passos. No entanto, informações como localização, dados pessoais e integração com redes sociais foram mencionadas com menor frequência, o que indica que há ainda certa limitação na compreensão mais ampla sobre o alcance da coleta de dados pelos smartwatches.

Quanto à **sensação de segurança e privacidade**, a pesquisa revelou uma relação direta entre o nível de escolaridade e a preocupação com esses aspectos. Participantes com maior formação acadêmica tendem a demonstrar maior conscientização e preocupação com os riscos envolvidos, enquanto usuários com menor escolaridade se mostraram significativamente menos preocupados.

Ainda assim, mesmo entre os usuários mais frequentes, o nível de preocupação não se mostrou elevado. De maneira surpreendente, a alta frequência de uso do dispositivo não se correlaciona com um aumento proporcional da preocupação com a privacidade, reforçando a hipótese de que muitos usuários encaram os riscos como um “mal necessário” para usufruir das funcionalidades oferecidas.

A análise por faixa etária reforçou a importância do contexto de uso na percepção de valor do smartwatch: usuários mais jovens valorizam a conectividade e o estilo, enquanto usuários mais velhos priorizam o monitoramento da saúde. Essa

diferença também pode influenciar a forma como cada grupo percebe os riscos relacionados à privacidade e segurança.

Em síntese, os resultados da pesquisa apontam que, embora exista algum nível de consciência sobre os dados coletados, essa consciência é parcial e muitas vezes não gera uma reação crítica por parte do usuário. A maioria dos participantes continua utilizando o dispositivo mesmo ciente da ausência de total transparência, o que revela uma tensão entre conveniência tecnológica e valores éticos.

Nesse sentido, torna-se ainda mais preocupante quando se consideram os riscos já identificados em relação aos smartwatches. O monitoramento contínuo pode gerar sensação de vigilância permanente e insegurança quanto à extensão dos dados coletados; o compartilhamento de informações com terceiros levanta preocupações sobre uso indevido para fins de publicidade direcionada; e a retenção prolongada dos dados aumenta a vulnerabilidade a ataques cibernéticos. Além disso, é possível que invasores explorem brechas para acessar dados pessoais e financeiros, praticar roubo de identidade, rastrear a localização dos usuários e até comprometer sua segurança física.

Essas descobertas reforçam a necessidade de que o design de artefatos digitais, como os smartwatches, considere de forma mais responsável e acessível os aspectos éticos relacionados à segurança e privacidade. É fundamental que fabricantes e desenvolvedores promovam práticas mais transparentes de coleta e tratamento de dados, além de investir em comunicação clara com seus usuários, considerando diferentes perfis etários e níveis de escolaridade.

7. RECOMENDAÇÕES ÉTICAS

A partir dos resultados obtidos neste estudo, foi desenvolvida uma cartilha de recomendações para o design ético de wearables, que constitui a principal contribuição desta pesquisa para o campo do design. Essa proposta, que pode ser encontrada no Anexo C e disponibilizada no [Google Drive](#), tem como finalidade orientar e facilitar a aplicação prática dos achados no cotidiano de designers e desenvolvedores, de modo a mitigar os problemas relacionados à falta de privacidade dos usuários e a nortear a criação de soluções mais éticas e socialmente responsáveis.

8. DIFICULDADES E LIMITAÇÕES DA PESQUISA

A realização desta pesquisa enfrentou alguns desafios que impactaram a obtenção dos resultados. Um dos principais obstáculos foi alcançar uma quantidade expressiva de respostas, superior a 385, o que exigiu a divulgação do questionário em redes sociais. Essa estratégia, entretanto, resultou em um viés geográfico, uma vez que a maior parte dos participantes residia na região Nordeste. Para minimizar essa limitação, a pesquisa foi também direcionada a universidades federais e estaduais, ampliando o alcance para outros estados. Como consequência dessa medida, contudo, verificou-se uma concentração do perfil dos respondentes em universitários, graduados e, em sua maioria, jovens, o que constitui outra limitação da investigação.

Apesar desses vieses, a pesquisa mantém sua relevância em função dos resultados obtidos e da contribuição que oferece para o debate acerca da ética em wearables. Ressalta-se, nesse sentido, que a discussão sobre ética em dispositivos vestíveis ainda se encontra em estágio inicial, de modo que este estudo não representa a finalização do tema, mas um passo dentro de um campo em construção.

9. TRABALHOS FUTUROS

Como perspectiva para trabalhos futuros, recomenda-se a realização de investigações mais aprofundadas sobre a chamada *conveniência digital*, fenômeno observado através da presente pesquisa, no qual os usuários embora não se sintam seguros em relação à proteção de suas informações pessoais, abrem mão da segurança e privacidade em troca do uso frequente do dispositivo. Torna-se relevante compreender as razões que originam e sustentam esse comportamento, como forma explorar estratégias de design capazes de mitigar tais riscos e promover escolhas mais seguras.

Além disso, sugere-se o desenvolvimento de estudos voltados para identificar formas mais adequadas de realizar o consentimento informado, analisando como os usuários interagem com os dispositivos em seus diferentes contextos de uso. Por fim, indica-se como caminho relevante a formulação de diretrizes éticas mais abrangentes, que considerem não apenas os smartwatches, mas também dispositivos vestíveis em geral.

REFERÊNCIAS

ADAM, A. Ethics for things. *Ethics and Information Technology*, v. 10, n. 2–3, p. 149–154, set. 2008.

ALEXANDER, L.; MOORE, M. Deontological Ethics. *Stanford Encyclopedia of Philosophy*. Disponível em: <https://plato.sydney.edu.au/entries/ethics-deontological/>. Acesso em: 24 set. 2024.

ALLHOFF, F.; HENSCHKE, A. The Internet of Things: Foundational ethical issues. *Internet of Things (Netherlands)*, v. 1–2, p. 55–66, 1 set. 2018.

AMAZON. *Mais vendidos: Wearables e tecnologia vestível - os mais vendidos na Amazon.com.br*. Disponível em: <https://www.amazon.com.br/gp/bestsellers/electronics/16243802011>. Acesso em: 7 set. 2024.

ANÁLISE EXPLORATÓRIA para Dados com Escala Likert. Direção: Isadora Lupchinski. Produção: Estatística na Prática. [S.l.: s.n.], 2020. Disponível em: https://www.youtube.com/watch?v=6-xpKe00TzY&ab_channel=Estat%C3%ADstica+na+pr%C3%A1tica. Acesso em: 31 maio 2024.

ARIAS, O. et al. Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems*, v. 1, n. 2, p. 99–109, 1 jun. 2015.

ATLAM, H. F.; WILLS, G. B. IoT Security, Privacy, Safety and Ethics. In: *DIGITAL Twin Technologies and Smart Cities*. [S.l.: s.n.], 2019. p. 123-149. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-18732-3_8. Acesso em: 23 out. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Glossário ANPD. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd>. Acesso em: 20 set. 2024.

BEG, Heebatullah et al. Enhancing Security and Data rates of Smartwatches. 2023. Monografia (Department of Electrical and Computer Engineering) - University of Victoria, [S.l.], 2023. Disponível em: <https://www.researchgate.net/publication/370493585>. Acesso em: 19 mar. 2024.

BEG, M.; KHAN, N.; IQBAL, M. Privacy in wearable devices: A systematic literature review. *Journal of Network and Computer Applications*, v. 213, p. 103536, 2023.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 15 ago. 2018. Seção 1, p. 1.

CARVALHO, Fernanda Potiguara. O ser atrás do dado: limites e desafios da anonimização e seus reflexos nos requisitos estabelecidos pela LGPD. 2024. Universidade de Brasília, 2024. Disponível em: http://www.rlbea.unb.br/jspui/bitstream/10482/48043/1/2021_FernandaPotiguaraCarvalho.pdf. Acesso em: 20 set. 2024.

CECCHINATO, M. E.; COX, A. L.; BIRD, J. Smartwatches: The good, the bad and the Ugly? *Conference on Human Factors in Computing Systems - Proceedings*. Anais... Association for Computing Machinery, 18 abr. 2015. Disponível em: <https://openaccess.city.ac.uk/id/eprint/16616/1/>. Acesso em: 7 ago. 2023.

CESAR, Zoraya. O jogador: 2ª parte. *Crônica do Dia*, 2018. Disponível em: <https://www.cronicadodia.com.br/2018/05/o-jogador-2a-parte-zoraya-cesar.html>. Acesso em: 21 set. 2024.

CHANNEL 360o. Estudo indica retomada do mercado de wearables no Brasil. Disponível em: <https://www.channel360.com.br/estudo-indica-retomada-do-mercado-de-wearables-com-aumento-de-64-nas-vendas-do-2o-trimestre/>. Acesso em: 7 set. 2024.

CHOUDHURY, Avishek; SHAMSZARE, Hamid. Investigating the Impact of User Trust on the Adoption and Use of ChatGPT: Survey Analysis. *JOURNAL OF MEDICAL* [incompleto].

COTE, Mark; SEYMOUR, William; PYBUS, Jennifer; MARIASIN, Dalia. *A review of the risks and psychological harms presented by consumer IoT products*. Department for Science, Innovation and Technology, 5 dez. 2024. Disponível em: https://assets.publishing.service.gov.uk/media/672b676dfbd69e1861921c21/A_review_of_the_risks_and_psychological_harms_presented_by_consumerIoT_products_-_Cote_et_al.pdf. Acesso em: 3 set. 2025.

CYBERSEC BRAZIL. *SmartAttack: nova técnica usa smartwatches para roubar dados de sistemas isolados via sinal ultrassônico*. 11 jun. 2025. Disponível em: <https://www.cybersecbrazil.com.br/post/smartattack-nova-t%C3%A9cnica-usa-smartwatches-para-roubar-dados-de-sistemas-isolados-via-sinal-ultrass%C3%B4>. Acesso em: 3 set. 2025.

DADOS PARA QUÊ?. Afinal, quais informações o seu smartwatch sabe sobre você?. [S.l.], 26 jul. 2021. Disponível em:

<https://dadospraque.com.br/dicas/afinal-quais-informacoes-o-seu-smartwatch-sabe-sobre-voce/>. Acesso em: 26 out. 2023.

DOS SANTOS, R. DESIGN PARA CONFIANÇA: A Experiência do Usuário com o Banco Digital. [S.l: s.n.] 2018.

ELOFSON, Erik. Trust, power and control in the implementation of collaborative IS. In: BURSTEIN, Frank; HOLSAPPLE, Clyde W. (Org.). *Cooperative Systems Design*. Dordrecht: Springer, 2013. p. 87-107. DOI: 10.1007/978-94-017-3614-5_6.

FALBE, Trine; FREDERIKSEN, Martin Michael; ANDERSEN, Kim. *The Ethical Design Handbook*. Freiburg: Smashing Media AG, 2020.

SHAHAKI, A.; HAUGEN, Ø. Social ethics in Internet of Things: An outline and review. [s.l: s.n.].

FAWLE, H.; LEBLANC, D. Smartwatch Vulnerability Analysis: Focusing on Bluetooth Low Energy. [S.l: s.n.] 2024.

FLORIDI, L. Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, v. 376, n. 2133, 28 nov. 2018.

FLORIDI, L.; TADDEO, M. What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Royal Society of London, 28 dez. 2016.

FURNELL, S. M.; JUSOR, A.; KATSABAS, D. The challenges of understanding and using security: A survey of end-users. *Computers and Security*, [S.l.], 2006. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404805002038?fr=RR-2&ref=pdf_download&rr=8873b8370e86273d. Acesso em: 29 mar. 2024.

GAF, B. M.; EMERY, W. Legal Issues with Wearable Technology. [S.l: s.n.]. Disponível em: <www.computer.org/computer-multimedia>.

GCF GLOBAL. Wearables: Pros and Cons of Wearable Technology. Disponível em: <https://edu.gcfglobal.org/en/wearables/pros-and-cons-of-wearable-technology/1/>.

GERHARDT, Tatiana; SILVEIRA, Denise. Métodos de Pesquisa. [S.l.]: PLAGEDER, 2009. ISBN 8538600710, 9788538600718. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=dRuzRyElzmkC&oi=fnd&pg=PA9&dq=classifica%C3%A7%C3%A3o+de+pesquisa&ots=94ObU2InKC&sig=WQwKelOLgDPWtoS7GMPllw_kodc#v=onepage&q=classifica%C3%A7%C3%A3o%20de%20pesquisa&f=false. Acesso em: 12 nov. 2023.

GLOBALYO. Revolutionizing connectivity: introducing the digital SIM for smartwatches. Disponível em: <https://www.globalyo.com/pt/revolutionizing-connectivity-introducing-the-digital-sim-for-smartwatches/>. Acesso em: 1 out. 2024.

GONZALEZ DE GOMEZ, M. *A ética da informação nas trilhas da filosofia.* Disponível em: <http://eprints.rclis.org/42284/1/A%20%C3%89tica%20da%20Informa%C3%A7%C3%A3o%20de%20Luciano%20Floridi%20nas%20Trilhas%20da%20Filosofia.pdf>. Acesso em: 24 set. 2024.

GUSENBAUER, Michael; HADDAWAY, Neal R. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Research Synthesis Methods*, v. 11, n. 2, p. 181-217, 2020. DOI: <https://doi.org/10.1002/jrsm.1378>.

HADDAWAY, Neal R.; COLLINS, Alexandra M.; COUGHLIN, Deborah; KIRK, Stuart. The role of Google Scholar in evidence reviews and its applicability to grey literature searching. *PLOS ONE*, v. 10, n. 9, e0138237, 2015. DOI: <https://doi.org/10.1371/journal.pone.0138237>.

HAJIBABAEI, N.; NAIK, K. Enhancing Security and Data rates of Smartwatches. 2023.

HANSON, K. Who's Behind the Orders your Smartwatch Is Giving You? Disponível em: <https://kshanson.medium.com/whos-behind-the-orders-your-smartwatch-is-giving-you-71f552e828e3>. Acesso em: 5 nov. 2023.

HARDIN, R. UZ on Trust Trustworthiness. 2002.

HENRIQUE, G. FUNÇÕES E LIMITES DA LGPD ENQUANTO INSTRUMENTO ESTATAL PARA PROTEÇÃO DO DIREITO À PRIVACIDADE. São Paulo: [s.n.]. Disponível em: <https://adelfa-api.mackenzie.br/server/api/core/bitstreams/8f6b4334-b240-4057-adf6-c26b8b07d126/content>. Acesso em: 20 set. 2024.

HOW Designers Destroyed the World - Mike Monteiro, at USI. Direção: USI Events. Intérprete: Mike Monteiro. [S. l.: s. n.], 2015. Disponível em: https://www.youtube.com/watch?v=qlcM21l61TE&ab_channel=USIEvents. Acesso em: 5 ago. 2024.

IBIRICU, B; VAN DER MADE, M. *Ethics by design: a code of ethics for the digital age.* *Journal of Information, Communication and Ethics in Society*, [s.l.], v. 18, n. 3, p.

387–404, 2020. Emerald Publishing. Disponível em: <https://doi.org/10.1108/JICES-11-2019-0121>. Acesso em: 15 maio 2025.

IBM. Linux on a Wrist Watch 1998-2001. [S.l.], 2001. Disponível em: https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=6102. Acesso em: 19 out. 2023.

JANEČEK, V. Ownership of personal data in the Internet of Things. *Computer Law and Security Review*, v. 34, n. 5, p. 1039–1052, 1 out. 2018.

KARAKAYA, Murat et al. How Secure is Your Smart Watch?. *International Journal of Information Security Science*, [s. l.], 2016. Disponível em: <https://dergipark.org.tr/tr/download/article-file/2160226>. Acesso em: 19 mar. 2024.

KOOHANG, Alex; FLOYD, Kevin; YERBY, Johnathan; PALISZKIEWICZ, Joanna. Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. *Issues in Information Systems*, [s. l.], 2021. Disponível em: https://iacis.org/iis/2021/2_iis_2021_136-149.pdf. Acesso em: 1 abr. 2024.

LAPOLA, Fernanda et al. Uma análise da segurança do protocolo Bluetooth Low Energy aplicado a dispositivos IoT vestíveis. [S.l: s.n.], 2018.

LAPOLA, Fernanda et al. Análise do Protocolo Bluetooth Low Energy Aplicado a Wearables IoT. *Revista de Sistemas e Computação*, v. 8, n. 1, p. 67-77, 2018.

LARICCHIA, F. Wearables shipments worldwide 2014-2023 | Statista. Disponível em: <https://www.statista.com/statistics/437871/wearables-worldwide-shipments/>.

LEBRETON, J. R.; ETZEL, J. A. Liking Likes: The Role of Social Media in Shaping Consumer Preferences. *Journal of Consumer Psychology*, v. 27, n. 3, p. 432–440, 2017.

LOPES, A. Hiperconectividade cotidiana. *Enciclopédia da Conscienciologia*, [S. l.], p. 7, 13 jan. 2016. Disponível em: <http://www.reposicons.org/bitstream/123456789/4941/1/Hiperconectividade-Cotidian a.pdf>. Acesso em: 30 out. 2023.

LOPES, C. A. Considerações sobre a ética. *Professare*, [S. l.], v. 6, n. 3, 2018. DOI: 10.33362/professare.v6i3.1342. Disponível em: <https://periodicos.uniarp.edu.br/index.php/professare/article/view/1342>. Acesso em: 24 set. 2024.

LOWENS, B.; MOTTI, V. G.; CAINE, K. Wearable Privacy: Skeletons in the Data Closet. *Proceedings - 2017 IEEE International Conference on Healthcare*

Informatics, ICHI 2017. Anais...Institute of Electrical and Electronics Engineers Inc., 8 set. 2017.

MJV INNOVATION. Cultura data-driven: personalização de serviços através dos dados. Disponível em: <https://www.mjvinnovation.com/pt-br/blog/cultura-data-driven-personalizacao-de-servicos-atraves-dos-dados/>. Acesso em: 1 out. 2024.

MALAGUTI, S. F. Privacidade e proteção de dados em dispositivos vestíveis. *Revista de Direito, Estado e Telecomunicações*, v. 12, n. 1, 2020.

MARENGO, L. L. et al. Mobile technologies in healthcare: reflections on development, application, legal aspects, and ethics. *Revista Panamericana de Salud Publica/Pan American Journal of Public Health*, v. 46, 2022.

MAYO, R. et al. Privacy in smartwatches: a review. *Journal of Information Privacy and Security*, v. 15, n. 4, p. 290–308, 2019.

MOK, T. M.; CORNISH, F.; TARR, J. Too Much Information: Visual Research Ethics in the Age of Wearable Cameras. *Integrative Psychological and Behavioral Science*, v. 49, n. 2, p. 309–322, 1 maio 2015.

MONTEIRO, M. A Designer's Code of Ethics. 2017 Disponível em: <<https://deardesignstudent.com/a-designers-code-of-ethics-f4a88aca9e95>>. Acesso em: 26 set. 2023.

MONTEIRO, M. *Ruined by Design: How Designers Destroyed the World, and What We Can Do to Fix It*. San Francisco: Mule Design, 2019.

MORADI, P. et al. A survey on privacy and security in wearable devices. *Journal of Network and Computer Applications*, v. 139, p. 72-90, 2019.

MOTTA, F.; SALGADO, A. R. Wearable Device Data Security. [S.l.: s.n.], 2022.

NASKAR. *Data security concerns in wearable devices*. 2024. Disponível em: <https://www.naskar.io/>. Acesso em: 3 set. 2025.

NIELSEN, Jakob. *The Role of Design Ethics in UX*. Nielsen Norman Group, 2021. Disponível em: <https://www.nngroup.com/videos/design-ethics-ux/>. Acesso em: 28 maio 2025.

NORMAN, D. A. *Emotional Design: Why We Love (or Hate) Everyday Things*. Basic Books, 2004.

NORMAN, D. A. *The Design of Everyday Things*. Basic Books, 2013.

OLIVEIRA, Jayne Silva de; TEIXEIRA, João Marcelo Xavier Natário. Ethical guidelines related to wearable devices: a literature review. In: ACM INTERNATIONAL CONFERENCE ON INTERACTIVE MEDIA EXPERIENCES WORKSHOPS (IMXW), 25. , 2025, Niterói/RJ. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025 . p. 76-80. DOI: <https://doi.org/10.5753/imxw.2025.1655>.

PAPANEK, V. (1971). Design for the real world.

PAUL, J. et al. Behaviour change: The impact of consumer trust on product purchase decision making. *Sebelas Maret Business Review*, v. 9, n. 1, p. 31–38, 2024.

PEREIRA, Luiz Carlos; MENDES, Paulo V. Internet das coisas (IoT): segurança e privacidade na era dos dispositivos conectados. *Revista Eletrônica de Sistemas de Informação*, v. 19, n. 1, p. 23-34, 2020.

PEREZ, A. J.; ZEADALLY, S. Privacy Issues and Solutions for Consumer Wearables. *IT Professional*, v. 20, n. 4, p. 46–56, 1 jul. 2018.

PICHON, R. Designing ethics for AI and wearables: challenges and opportunities. *AI & Society*, v. 35, n. 3, p. 621–630, 2020.

PINTO, J. M. et al. Segurança e privacidade em dispositivos vestíveis: um estudo sistemático. *Journal of Information Systems and Technology Management*, v. 17, 2020.

PLOGSTIES, E.; PROFESSOR, S.; BRINO, V. Balancing Wearables in the Workplace: Protecting Privacy and Human Rights-a Legal Analysis within the European Legal Framework. [s.l: s.n.].

PORITIU, T. Smartwatch Privacy Risks: Safeguard Your Wearables in 2024. Disponível em: <https://vpnoverview.com/privacy/devices/privacy-risks-smartwatch/>. Acesso em: 5 nov. 2023.

PORTER, J. An overview of ethics for IoT devices. *Ethics in Technology Review*, v. 12, n. 2, p. 110-120, 2021.

QU, S.; GAO, X. Analysis of Ethical Issues Involved in Wearable Equipment for Health Care. Proceedings - 2020 International Conference on Public Health and Data Science, ICPHDS 2020. Anais...Institute of Electrical and Electronics Engineers Inc., 1 nov. 2020.

REPUBLIC OF IRELAND. Data Protection Act 2018. [S.l.: s.n.], 2018.

ROBINSON, S. et al. Usability and trust in wearable health technology: a systematic review. *Computers in Human Behavior*, v. 99, p. 126-139, 2019.

ROOSSIEN, C. C. et al. Ethics in Design and Implementation of Technologies for Workplace Health Promotion: A Call for Discussion. *Frontiers in Digital Health*, v. 3, 20 ago. 2021.

SALUTES, Bruno. Para que servem os sensores de um smartwatch?. [S. l.], 26 jul. 2021. Disponível em: <https://canaltech.com.br/smartwatch/para-que-servem-os-sensores-de-um-smartwatch/>. Acesso em: 29 out. 2024.

SANTOS, L. A.; MENDES, R. Ethical considerations for wearable device design. *Journal of Ethics in Information Technology*, v. 18, n. 3, p. 201-215, 2021.

SANTOS, L. S.; SERAFIM, M. C. Decisão ética na administração pública: perspectivas práticas a partir da ética normativa e descritiva. *Gestão & Planejamento*, v. 24, p. 4–20, 2023.

SCHWEITZER, A. THE EVOLUTION OF ETHICS. [s.l.: s.n.]. Disponível em: <https://www.theatlantic.com/magazine/archive/1958/11/the-evolution-of-ethics/642820/>. Acesso em: 22 mar. 2024.

SENEVIRATNE, S. et al. A Survey of Wearable Devices and Challenges. *IEEE Communications Surveys and Tutorials* Institute of Electrical and Electronics Engineers Inc., , 1 out. 2017.

SINGH, P.; GUPTA, S. Security risks in wearable computing: a comprehensive review. *Journal of Computer Security*, v. 28, n. 1, p. 123-152, 2020.

SMITH, J. Trust and privacy in wearable devices. *Journal of Information Security*, v. 11, n. 4, p. 254-267, 2017.

SORRI, K.; MUSTAFEE, N.; SEPPÄNEN, M. Revisiting IoT definitions: A framework towards comprehensive use. *Technological Forecasting and Social Change*, v. 179, 1 jun. 2022.

SOUZA, Clarisse. Vida na Era da Hiperconectividade. *SERG*, [S. l.], p. 15, 1 abr. 2021. Disponível em: <http://www.hcc.inf.puc-rio.br/EMAPS/userfiles/downloads/Resenha-Floridi2015.pdf>. Acesso em: 20 out. 2023.

SOUSA, D. Análise das diretrizes éticas para segurança em wearables. *Revista Brasileira de Ética em Computação*, v. 5, n. 1, p. 45-59, 2022.

SUI, A. et al. Ethical considerations for the use of consumer wearables in health research. *Digital Health*, v. 9, 1 jan. 2023.

TADDEO, M. Ethics, Technology, and Internet of Things. *Philosophical Transactions of the Royal Society A*, v. 376, n. 2133, 2018.

TAYUNG, D. Socratic concept of ethics and it's relevance in practical life. JETIR, 2019. Disponível em: <https://www.jetir.org/papers/JETIR1908793.pdf>. Acesso em: 14 jan. 2024.

TEIXEIRA, F. *Os 10 princípios de um bom design, segundo Dieter Rams*. Medium – UX Design Brasil, 19 abr. 2012. Disponível em: <https://brasil.uxdesign.cc/os-10-princ%C3%ADpios-de-um-bom-design-segundo-diet-er-rams-8b45e4fa3e03>. Acesso em: 26 maio 2025.

TRE. O que são dados pessoais?. [S. l.], 2020. Disponível em: <https://www.tre-pr.jus.br/transparencia-e-prestacao-de-contas/lei-geral-de-protecao-d-e-dados/o-que-sao-dados-pessoais>. Acesso em: 28 ago. 2024.

Trevino, L. K., & Nelson, K. A. *Managing business ethics: Straight talk about how to do it right*, 2021. Acesso em: 03 abr. 2025

TZAFESTAS, S. G. Ethics and law in the internet of things world. *Smart CitiesMDPI*, 1 dez. 2018.

UFPE. Perguntas e Respostas Frequentes ao CEP. [S. l.], 2016. Disponível em: <https://www.ufpe.br/documents/619819/801156/Perguntas+e+Respostas+Frequentes+CEP+UFPE.pdf/7b4f1d31-eed0-4c7f-8815-9d0b7bad7db9>. Acesso em: 7 mar. 2024.

USP. Site de estatística. [S. l.], 2024. Disponível em: <http://estatistica.bauru.usp.br/calculoamostral/index.php>. Acesso em: 5 ago. 2024.

VAN DEN HOF, S.; PERSAD, G. Ethical issues in wearable technology: A literature review. *Journal of Information Ethics*, v. 29, n. 1, p. 5-19, 2020.

YANG, C. et al. An Empirical Study on the Data Security and Privacy Awareness to Use Health Care Wearable Devices. IEEE, 2019.

YANG, M.; GUO, J.; BAI, L. A Data Privacy-preserving Method for Students' Physical Health Monitoring by Using Smart Wearable Devices. IEEE, p. 29–34, 2020.

WALKING the tightrope between data sharing and data protection. *Nature Medicine*, v. 28, n. 5, p. 873, 1 maio 2022.

WANG, Isabelle. Using Smartwatches to Improve Health and Wellness. GMU, [S. l.], p. 16, 27 fev. 2017. Disponível em: http://copyright.gmu.edu/?page_id=301. Acesso em: 19 mar. 2024.

WANG, Y. The Design Dilemma of Personalized Health Applications: the Balance Between Meeting User Needs and Data Security. European Alliance for Innovation n.o., 17 jun. 2024.

ZILLIG, F. *Ética e Design: uma conversa necessária*. UX Collective Brasil, 17 abr. 2019. Disponível em: <https://brasil.uxdesign.cc/%C3%A9tica-e-design-uma-conversa-necess%C3%A1ria-d10f4ee6565e>. Acesso em: 28 maio 2025.

APÊNDICE A - Formulário de teste

O presente formulário foi elaborado inicialmente no andamento da pesquisa e testado com um grupo de usuários voluntários. Conforme explicado anteriormente e poderá ser observado pelo teor das questões, este formulário se enquadra como questionário de opinião pública. Por isso, esse formulário não foi submetido ao Comitê de Ética, sendo apresentado neste anexo somente como forma de comparação com a nova versão, que realiza coleta de dados pessoais dos participantes.

Figura A1 - Capa do questionário, explicações gerais e termo de responsabilidade

Design Ético em Smartwatches
percepção dos usuários acerca de segurança e transparência dos dados coletados

Smartwatches são éticos?

Olá!
Sou Jayne, mestranda em Design de Artefatos Digitais pela Universidade Federal de Pernambuco (UFPE).
Minha pesquisa visa investigar a opinião dos usuários a respeito da ética nos smartwatches. Para isso, o objetivo deste formulário é identificar a sua visão a respeito da ética e segurança dos dados coletados em seu dispositivo.

O que é necessário para participar da pesquisa

- Ter sido/Ser usuário de smartwatch
- Ter disponibilidade de no máximo 10 min para responder essa pesquisa

Termo de Responsabilidade dos Dados da Pesquisa
Os dados coletados com este formulário e com a pesquisa de modo geral são responsabilidade da pesquisadora em questão.

Para este formulário

✓ Coletaremos ✓

- ✓ Informações demográficas como a região onde mora, idade e gênero, para verificar se há algum foco de público na pesquisa.
- ✓ Sua opinião sobre os smartwatches para realizar o mapeamento
- ✓ Sua opinião sobre a pesquisa em si, pois esta é uma pesquisa de teste.

✗ Não coletaremos ✗

- ✗ Informações pessoais ou sensíveis, como nome, cargo, local onde trabalha, telefone, raça entre outros
- ✗ Não realizaremos gravações ou coleta da imagem dos usuários participantes

jayne.oliveira@ufpe.br [Mudar de conta](#)

🔒 Não compartilhado

* Indica uma pergunta obrigatória

Figura A2 - Consentimento do participante e filtragem inicial

Você leu e concorda com o Termo de Responsabilidade anteriormente citado? *

Sim

Não

Você usa/já utilizou algum smartwatch?

Sim

Não

Figura A3 - Mapeamento das características demográficas do participante

Informações demográficas

Qual a região onde você mora? *

Norte

Nordeste

Centroeste

Sudeste

Sul

Com que gênero você se identifica mais? *

Feminino

Masculino

Não-binário

Prefiro não dizer

Outro: _____

Qual a sua faixa etária?

menos que 18 anos

18 anos a 24 anos

25 anos a 34 anos

35 anos a 44 anos

45 anos a 54 anos

55 anos a 64 anos

mais que 64 anos

Figura A4 - Continuação das perguntas demográficas

Qual seu nível de escolaridade?

- Não frequentou a escola
- Ensino Fundamental Incompleto
- Ensino Fundamental Completo
- Ensino Médio Incompleto
- Ensino Médio Completo
- Ensino Superior Incompleto
- Ensino Superior Completo

Com que frequência você utiliza o seu smartwatch?

- Todos os dias
- Quase todos os dias
- 1 vez por semana
- Para realizar atividades específicas
- Raramente lembro de usar

Com que objetivo você geralmente utiliza o seu smartwatch?

- Moda e estilo
- Monitorar a saúde
- Monitorar especificamente atividades físicas
- Ter mais praticidade, utilizando da conexão com outros dispositivos

[Voltar](#) [Próxima](#)  Página 2 de 4 [Limpar formulário](#)

Figura A5 - Questões relacionadas a percepção do usuário a respeito da ética, privacidade e segurança dos smartwatches

Ética dos smartwatches

Você poderia citar alguns dados que o seu relógio coleta a seu respeito? *

Sua resposta

Tenho **conhecimento total** sobre quais dados são coletados a meu respeito *

1 2 3 4 5

Discordo completamente Concordo completamente

Sempre sou informado sobre os dados que estão sendo utilizados *

1 2 3 4 5

Discordo completamente Concordo completamente

Utilizando o meu próprio smartwatch, sei onde posso **cancelar** o fornecimento dos meus dados pessoais *

1 2 3 4 5

Discordo completamente Concordo completamente

Me sinto completamente seguro utilizando esse dispositivo *

1 2 3 4 5

Discordo completamente Concordo completamente

Figura A6 - Continuação das questões sobre ética e experiência do usuário

Me sinto vigiado pelo meu smartwatch

1 2 3 4 5

Discordo completamente Concordo completamente

Me sinto incomodado quando meu smartwatch compartilha dados com outros dispositivos meus, como celular e computador, sem o meu consentimento ou ciência. *

1 2 3 4 5

Discordo completamente Concordo completamente

Percebo que não consigo me sentir a vontade quando utilizo o meu smartwatch *

1 2 3 4 5

Discordo completamente Concordo completamente

Deixo de realizar certas atividades quando estou utilizando o meu smartwatch *

1 2 3 4 5

Discordo completamente Concordo completamente

Você tem algum comentário ou vivência que deseja compartilhar sobre o uso de smartwatches?

Sua resposta

[Voltar](#) [Próxima](#)  Página 3 de 4 [Limpar formulário](#)

Figura A7 - Questões sobre a experiência do participante com o questionário

Opinião sobre a pesquisa

Estamos quase no fim da pesquisa. Muito obrigada por ter chegado até aqui!

O que você achou da pesquisa?

- Deveria ter menos perguntas
- Pouco objetiva
- Levei muito tempo para responder
- Nenhuma das alternativas acima

Gostaria de deixar algum comentário?

Sua resposta

[Voltar](#) [Enviar](#) [Página 4 de 4](#) [Limpar formulário](#)

APÊNDICE B - Formulário da pesquisa qualitativa

Conforme explicado anteriormente, o formulário mostrado a seguir corresponde ao que será submetido para a avaliação do Comitê de Ética e só foi aplicado após a devida autorização.

Figura B1 - Capa do questionário e breve explicação sobre a pesquisa

Design ético de wearables:
Investigando a experiência do usuário sobre ética, privacidade e segurança em smartwatches

Smartwatches são éticos?

Olá!
Sou Jayne, mestranda em Design de Artefatos Digitais pela Universidade Federal de Pernambuco (UFPE).

Minha pesquisa visa investigar a opinião dos usuários a respeito da ética nos smartwatches. Para isso, o objetivo deste formulário é identificar a sua visão a respeito da ética e segurança dos dados coletados em seu dispositivo.

jayne.oliveira@ufpe.br [Mudar de conta](#)

* Indica uma pergunta obrigatória

Enviar por e-mail *

Registrar jayne.oliveira@ufpe.br como o e-mail a ser incluído na minha resposta

Próxima Página 1 de 4 [Limpar formulário](#)

O usuário terá acesso ao Termo de Consentimento Livre e Informado através do clique no link do documento, disponibilizado no próprio formulário, conforme mostra o Anexo B. Após a leitura, ele poderá consentir ou não através da resposta relacionada a isso no próprio formulário. A Figura 9 demonstra a estrutura do formulário.

Figura B2 - Acesso ao termo de consentimento e autorização do usuário

Termo de consentimento

Acesse aqui o termo de consentimento para se informar sobre o objetivo da pesquisa, os riscos e benefícios de participar dela.

[Termo de consentimento](#)

Você leu e concorda com o Termo de Consentimento anteriormente citado? *

Sim, aceito participar da pesquisa

Não, não aceito participar da pesquisa

Você usa/já utilizou algum smartwatch? *

Sim

Não

[Voltar](#) [Próxima](#)  Página 2 de 4 [Limpar formulário](#)

Figura B3 - Informações demográficas

Informações demográficas

Qual a região onde você mora?

Norte

Nordeste

Centroeste

Sudeste

Sul

Com que gênero você se identifica mais?

Feminino

Masculino

Não-binário

Prefiro não dizer

Outro: _____

Qual a sua faixa etária?

menos que 18 anos

18 anos a 24 anos

25 anos a 34 anos

35 anos a 44 anos

45 anos a 54 anos

55 anos a 64 anos

mais que 64 anos

Figura B4 - Continuação das perguntas demográficas

Qual seu nível de escolaridade?

- Não frequentou a escola
- Ensino Fundamental Incompleto
- Ensino Fundamental Completo
- Ensino Médio Incompleto
- Ensino Médio Completo
- Ensino Superior Incompleto
- Ensino Superior Completo

Como você classifica o seu nível de familiaridade com tecnologias em geral?

- Iniciante, apenas uso básico do dia a dia, com supervisão
- Intermediário, confortável com uso de tecnologia e sei resolver problemas pequenos sozinho
- Avançado, tenho domínio e consigo aprender a utilizar por conta própria

Qual o modelo/marca do seu smartwatch?

Sua resposta _____

Com que frequência você utiliza o seu smartwatch?

- Todos os dias
- Quase todos os dias
- 1 vez por semana
- Para realizar atividades específicas
- Raramente lembro de usar

Figura B5 - Parte final das perguntas demográficas

Com que objetivo você geralmente utiliza o seu relógio?

- Moda e estilo
- Monitorar a saúde
- Monitorar especificamente atividades físicas
- Ter mais praticidade, utilizando da conexão com outros dispositivos

[Voltar](#) [Próxima](#)  Página 3 de 4 [Limpar formulário](#)

Figura B6 - Perguntas sobre ética, segurança e privacidade dos usuários

Ética dos smartwatches

Você poderia citar alguns dados que o seu relógio coleta a seu respeito?

Sua resposta _____

Em geral, o quanto você se preocupa com a segurança e privacidade das informações que você respondeu na pergunta anterior? *

1 2 3 4 5

😊 Não tenho preocupação nenhuma 🤔 Me preocupo bastante

Tenho **conhecimento total** sobre quais dados são coletados a meu respeito

1 2 3 4 5

❌ Discordo completamente ✅ Concordo completamente

Sempre sou informado sobre os dados que estão sendo utilizados nos aplicativos disponíveis no relógio

1 2 3 4 5

❌ Discordo completamente ✅ Concordo completamente

Utilizando o meu próprio smartwatch, sei onde posso **cancelar** o fornecimento dos meus dados pessoais

1 2 3 4 5

❌ Discordo completamente ✅ Concordo completamente

Figura B7 - Continuação das perguntas relacionadas a ética

Sinto que meus dados pessoais estão seguros e protegidos					
1	2	3	4	5	
<input checked="" type="checkbox"/> Discordo completamente	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Concordo completamente

Me sinto completamente seguro utilizando esse dispositivo					
1	2	3	4	5	
<input checked="" type="checkbox"/> Discordo completamente	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Concordo completamente

Me sinto vigiado pelo meu smartwatch					
1	2	3	4	5	
<input checked="" type="checkbox"/> Discordo completamente	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Concordo completamente

Me sinto incomodado quando meu smartwatch compartilha dados com outros dispositivos meus, como celular e computador, sem o meu consentimento ou ciência.					
1	2	3	4	5	
<input checked="" type="checkbox"/> Discordo completamente	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Concordo completamente

Figura B8- Parte final do questionário

Percebo que não consigo me sentir a vontade quando utilizo o meu smartwatch

1 2 3 4 5

Discordo completamente Concordo completamente

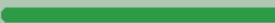
Deixo de realizar certas atividades quando estou utilizando o meu relógio

1 2 3 4 5

Discordo completamente Concordo completamente

Você tem algum comentário ou vivência que deseja compartilhar sobre o uso do dispositivo?

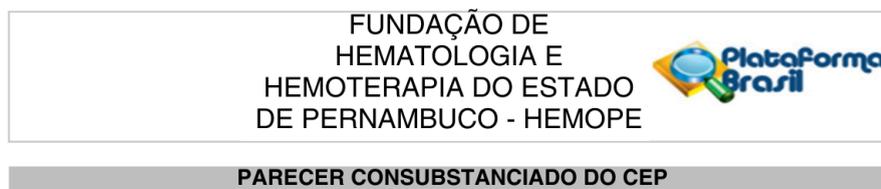
Sua resposta

[Voltar](#) [Enviar](#)  Página 4 de 4 [Limpar formulário](#)

ANEXO A - Parecer de aprovação do Comitê de Ética HEMOPE

O presente anexo corresponde à devida análise e aprovação do Comitê de Ética da Fundação de Hematologia e Hemoterapia de Pernambuco (HEMOPE), conforme ilustram as Figuras C1, C2, C3 e C4.

Figura C1 - Início de documento



DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: "DESIGN ÉTICO DE WEARABLES: investigando a experiência do usuário sobre ética, privacidade e segurança em smartwatches"

Pesquisador: JAYNE SILVA DE OLIVEIRA

Área Temática:

Versão: 1

CAAE: 85251624.8.0000.5195

Instituição Proponente: Fundação de Hematologia e Hemoterapia do Estado de Pernambuco -

Patrocinador Principal: Financiamento Próprio

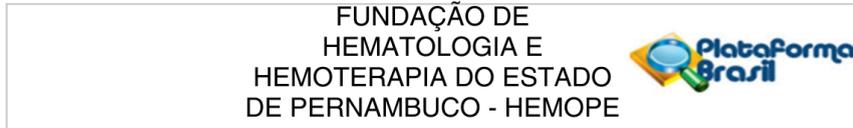
DADOS DO PARECER

Número do Parecer: 7.312.164

Apresentação do Projeto:

Projeto de dissertação, apresentado ao Programa de Pós Graduação em Design da Universidade Federal de Pernambuco, pela Mestranda Jayne Silva de Oliveira e orientado pelo Prof. Dr. João Marcelo Xavier Natário Teixeira. A pesquisa traz como tema o uso de wearable devices, ou vestíveis. O estudo objetiva mapear as opiniões dos usuários acerca da ética percebida por eles no uso de smartwatches e contribuir para o design e desenvolvimento de wearables mais éticos. A preocupação em realizar esse estudo vem do fato de que esses dispositivos são projetados para interagir com os usuários cotidianamente, coletando diversas informações pessoais como localização, hábitos de exercício, preferências de navegação, além de informações relacionadas à saúde como qualidade do sono, batimentos cardíacos, entre outros. Além disso, esses dispositivos possuem diversas vulnerabilidades de segurança e privacidade, o que expõe o usuário a constantes riscos. Trata-se de uma pesquisa qualitativa, o instrumento de coleta será um questionário composto por perguntas fechadas e abertas, aplicado por meio da plataforma online Google Forms. A coleta dos dados relata a segurança e privacidade da pesquisa virtual e pretende atingir uma amostra de 385 participantes. Critérios de Inclusão: ser usuário de smartwatch, ser brasileiro ou estar no Brasil; ser maior de 18 anos. Serão excluídos os participantes que possuem smartwatch, mas não fazem uso.

Figura C2 - Objetivos e riscos da pesquisa



Continuação do Parecer: 7.312.164

Objetivo da Pesquisa: OBJETIVOS Geral: Mapear o nível de conhecimento dos usuários a respeito dos dados coletados, bem como o quanto eles confiam em seus smartwatches. Além disso, visa identificar questões éticas que lhes causam preocupação e como tais quesitos afetam suas experiências de uso.

Específicos:

- ¿ Realizar uma revisão da literatura sobre as diretrizes e desafios éticos associadas ao uso de smartwatches;
- ¿ Desenvolver e validar um instrumento de pesquisa para medir o nível de confiança e ciência dos usuários de smartwatches;
- ¿ Coletar dados por meio de uma pesquisa quantitativa junto a uma amostra representativa de usuários;
- ¿ Analisar os dados coletados para identificar os principais fatores que influenciam a confiança deles e suas preocupações éticas relacionadas ao uso desses dispositivos;
- ¿ Investigar como essas preocupações éticas impactam a experiência de uso dos smartwatches pelos usuários.

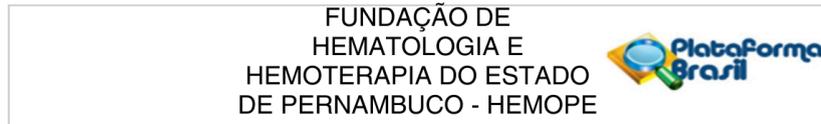
Avaliação dos Riscos e Benefícios:

Riscos:

Como riscos, a pesquisa envolve a coleta de informações demográficas que podem causar constrangimento ou desconfortos aos participantes. Como forma de amenizar esse risco, o participante terá a possibilidade de não responder as perguntas que não se sintam confortável. Outra medida adotada é a coleta de informações mais generalizadas como faixa etária ao invés de idade. Embora informações demográficas, como região do país e faixa etária, sejam coletadas, elas serão registradas de maneira a preservar o anonimato dos participantes, evitando a coleta de dados que possam identificá-los diretamente, como nome ou endereço residencial. Além dessas informações, o endereço de e-mail será coletado apenas para vincular as respostas dos participantes e evitar duplicações, sendo armazenado de maneira segura em dispositivo móvel protegido por senha e com acesso restrito à pesquisadora responsável. Ainda assim, existe um risco potencial relacionado à identificação caso os dados sejam indevidamente acessados ou vazados. Esse risco será minimizado pelo

Endereço: Rua Joaquim Nabuco, 171
Bairro: Graças **CEP:** 52.011-000
UF: PE **Município:** RECIFE
Telefone: (81)3182-4771 **E-mail:** cep@hemope.pe.gov.br

Figura C3 - Comentários e considerações



Continuação do Parecer: 7.312.164

uso de sistemas seguros de armazenamento e pela adesão à Lei Geral de Proteção de Dados (LGPD).

Benefícios:

Embora a participação não ofereça benefícios diretos aos participantes, o estudo contribuirá para o avanço do conhecimento sobre segurança e privacidade em dispositivos vestíveis, com foco na experiência do usuário. Os resultados podem influenciar o desenvolvimento de diretrizes éticas e soluções que promovam maior segurança e confiança no uso de smartwatches e outros dispositivos semelhantes.

Comentários e Considerações sobre a Pesquisa: O uso de Wearable se aplica a Tecnologia da Informação (TI). Esta é um conjunto de princípios morais que orientam o uso de sistemas de informação de forma responsável e que proteja a sociedade. A ética na TI abrange várias áreas, como: Privacidade e segurança, é fundamental respeitar a privacidade dos usuários e garantir a segurança das informações. Estudos com esses fins são pertinentes para segurança da manipulação de dados e respeito à segurança dos usuários.

Considerações sobre os Termos de apresentação obrigatória:

Projeto Detalhado Ok

TCLE- OK

Folha de Rosto -Ok

Cronograma Ok

Currículo lattes (pesquisador e orientador) Ok

Termo Compromisso e Confidencialidade - OK

Recomendações: Não se aplica

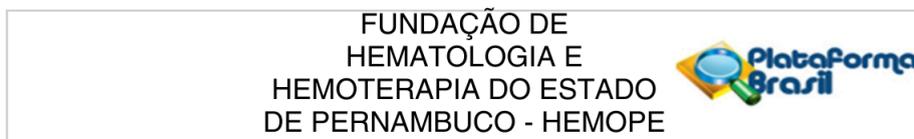
Conclusões ou Pendências e Lista de Inadequações:

Diante do exposto, o CEP- HEMOPE, de acordo com as atribuições definidas nas Resoluções CNS nº 466/12 e 510/2016, manifesta-se pela aprovação do projeto.

Considerações Finais a critério do CEP:

Lembramos que a pesquisadora responsável assume o compromisso de encaminhar ao CEP da Fundação Hemope o Relatório Final baseado na conclusão do estudo e na incidência de

Endereço: Rua Joaquim Nabuco, 171
Bairro: Graças **CEP:** 52.011-000
UF: PE **Município:** RECIFE
Telefone: (81)3182-4771 **E-mail:** cep@hemope.pe.gov.br

Figura C4 - Aprovação do Comitê

Continuação do Parecer: 7.312.164

publicações decorrentes deste, de acordo com o dispositivo nas normas vigentes, Resoluções da CNS nº 510/2016. O prazo de entrega do Relatório é de até 30 dias, após o encerramento da pesquisa.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMACOES_BASICAS_DO_PROJETO_2467660.pdf	03/12/2024 13:16:35		Aceito
Projeto Detalhado / Brochura Investigador	Projeto_detalhado_Jayne_corrigido.pdf	03/12/2024 13:16:02	JAYNE SILVA DE OLIVEIRA JAYNE SILVA DE OLIVEIRA	Aceito
Outros	declaracao_vinculo.pdf	29/11/2024 12:52:29	JAYNE SILVA DE OLIVEIRA	Aceito
Outros	InstrumentoDeColetaDeDados.pdf	29/11/2024 12:50:03	JAYNE SILVA DE OLIVEIRA	Aceito
Outros	Curriculo_lattes_Joao.pdf	29/11/2024 12:49:19	JAYNE SILVA DE OLIVEIRA	Aceito
Outros	Curriculo_lattes_Jayne.pdf	29/11/2024 12:49:01	JAYNE SILVA DE OLIVEIRA	Aceito
Outros	TermoCompromissoConfidencialidade.pdf	29/11/2024 12:48:31	JAYNE SILVA DE OLIVEIRA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLColetaVirtual_assinado.pdf	29/11/2024 12:48:09		Aceito
Folha de Rosto	folhaDeRosto_assinado.pdf	29/11/2024 12:46:47	JAYNE SILVA DE OLIVEIRA	Aceito

Situação do Parecer:

Aprovado

Necessita Apreciação da CONEP:

Não

RECIFE, 20 de Dezembro de 2024

Assinado por:
Maria Iraci Buarque Valença
(Coordenador(a))

Endereço: Rua Joaquim Nabuco, 171
Bairro: Graças **CEP:** 52.011-000
UF: PE **Município:** RECIFE
Telefone: (81)3182-4771 **E-mail:** cep@hemope.pe.gov.br

ANEXO B - Termo de Consentimento Livre e Esclarecido - Coleta De Dados Virtual

As Figuras D1 e D2 a seguir correspondem ao termo de consentimento a ser enviado às pessoas interessadas em participar da pesquisa. Elas deverão ler esse documento, a fim de obter conhecimento sobre o objetivo da pesquisa, riscos e benefícios de participar dela. Após a leitura, esses interessados deverão realizar o consentimento explícito através da resposta no questionário.

É importante salientar que, as informações referentes ao endereço e número de telefone da pesquisadora e orientador estavam disponíveis no documento original, mas foram ocultadas na Figura D1, devido à publicação da pesquisa e necessidade preservação de dados pessoais.

Figura D1 - Termo de Consentimento Livre e Esclarecido - Coleta de Dados Virtual

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO - COLETA DE DADOS VIRTUAL

Convidamos o (a) Sr. (a) para participar como voluntário (a) da pesquisa Design ético de wearables: investigando a experiência do usuário sobre ética, privacidade e segurança em wearables, que está sob a responsabilidade da pesquisadora Jayne Silva de Oliveira, com endereço [REDACTED] Pernambuco e CEP [REDACTED] - Telefone (81) [REDACTED] e e-mail (jayne.oliveira@ufpe.br) para contato do pesquisador responsável (inclusive ligações a cobrar), sob a orientação de: Prof. Dr. João Marcelo Xavier Natário Teixeira Telefone: (81) [REDACTED] e-mail (jmxnt@cin.ufpe.br).

Todas as suas dúvidas podem ser esclarecidas com o responsável por esta pesquisa. Apenas quando todos os esclarecimentos forem dados e você concorde em participar desse estudo, pedimos que assinala a opção de "Aceito participar da pesquisa" no final desse termo.

O (a) senhor (a) estará livre para decidir participar ou recusar-se. Caso não aceite participar, não haverá nenhum problema, desistir é um direito seu, bem como será possível retirar o consentimento em qualquer fase da pesquisa, também sem nenhuma penalidade.

INFORMAÇÕES SOBRE A PESQUISA:

- **Descrição da pesquisa:**
Esta pesquisa tem como objetivo compreender a percepção dos usuários de smartwatches sobre questões relacionadas à segurança e privacidade de dados coletados por esses dispositivos. Os resultados desta pesquisa poderão contribuir para o desenvolvimento de diretrizes e melhorias no design desses produtos, beneficiando a sociedade em geral.

Esclarecimento sobre a participação:
Sua participação consiste em responder a um questionário online, que será disponibilizado por meio da plataforma Google Forms. O questionário abordará questões gerais sobre o uso do smartwatch, sua experiência como usuário e suas percepções sobre segurança e privacidade. Além disso, o questionário contém perguntas relacionadas à sua características demográficas como faixa etária, região onde mora, entre outros. Essas informações são coletadas a fim de identificar vieses na pesquisa.

A coleta de dados será feita de forma virtual e individual. No formulário você **não** responderá a perguntas relacionadas a dados pessoais ou sensíveis, como nome, idade, documentações, entre outros. No entanto, seu email será coletado como forma de evitar que uma mesma pessoa responda duas vezes o mesmo questionário. Você poderá acessar o questionário por meio de um link enviado por e-mail ou rede social de sua preferência. O tempo estimado para responder às perguntas é de 10 a 15 minutos. Você poderá optar por não responder a qualquer questão, exceto se você possui um smartwatch/relógio inteligente e se você confia nele, pois essas perguntas são fundamentais para cumprir o objetivo da pesquisa. Ainda assim, você poderá encerrar sua participação a qualquer momento, sem prejuízo algum e solicitar à pesquisadora a exclusão das informações que você respondeu.

- **Riscos associados à pesquisa:**
Os potenciais riscos envolvem a coleta de um dado pessoal identificável: seu e-mail, necessário para garantir a organização das respostas e evitar duplicidade. Esse dado será armazenado em local seguro e utilizado exclusivamente para esta pesquisa. Além disso, medidas de segurança, como acesso restrito e uso de senhas, serão adotadas para minimizar riscos de exposição de informações. Não serão coletados outros dados que possam comprometer sua privacidade, como nome, endereço ou número de telefone.
- **Benefícios:**
Sua participação nesta pesquisa não oferecerá benefícios diretos a você. No entanto, contribuirá para o avanço do conhecimento sobre segurança e privacidade em dispositivos vestíveis, podendo gerar melhorias na experiência e na segurança de futuros usuários desses dispositivos.
- **Sigilo e confidencialidade:**
Todas as informações fornecidas serão tratadas com confidencialidade. Os dados coletados serão utilizados exclusivamente para fins de análise acadêmica e apresentados de forma agregada, sem qualquer possibilidade de identificação individual.

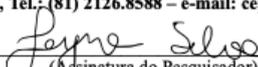
Esclarecemos que os participantes dessa pesquisa têm plena liberdade de se recusar a participar do estudo e que esta decisão não acarretará penalização por parte dos pesquisadores. Todas as informações desta pesquisa serão confidenciais e serão divulgadas apenas em eventos ou publicações científicas, não havendo identificação dos voluntários, a não ser entre os responsáveis pelo estudo, sendo assegurado o sigilo sobre a sua participação. Os dados coletados nesta pesquisa a saber, o email

Figura D2 - Continuação do Termo de Consentimento

pessoal, sob a responsabilidade da pesquisadora Jayne Silva de Oliveira no endereço acima informado, pelo período de mínimo 5 anos após o término da pesquisa.

Nada lhe será pago e nem será cobrado para participar desta pesquisa, pois a aceitação é voluntária, mas fica também garantida a indenização em casos de danos, comprovadamente decorrentes da participação na pesquisa, conforme decisão judicial ou extrajudicial. Se houver necessidade, as despesas para a sua participação serão assumidas pelos pesquisadores (ressarcimento de transporte e alimentação).

Em caso de dúvidas relacionadas aos aspectos éticos deste estudo, o (a) senhor (a) poderá consultar o Comitê de Ética em Pesquisa Envolvendo Seres Humanos da UFPE no endereço: **Avenida da Engenharia s/n – 1º Andar, sala 4 - Cidade Universitária, Recife-PE, CEP: 50740-600, Tel.: (81) 2126.8588 – e-mail: cephumanos.ufpe@ufpe.br.**


(Assinatura do Pesquisador)

CONSENTIMENTO DA PARTICIPAÇÃO DA PESSOA COMO VOLUNTÁRIO (A)

Eu, _____, CPF _____, abaixo assinado, após a leitura (ou a escuta da leitura) deste documento e de ter tido a oportunidade de conversar e ter esclarecido as minhas dúvidas com o pesquisador responsável, concordo em participar do estudo Design ético de wearables: investigando a experiência do usuário sobre ética, privacidade e segurança em wearables, como voluntário (a). Fui devidamente informado (a) e esclarecido (a) pelo(a) pesquisador (a) sobre a pesquisa, os procedimentos nela envolvidos, assim como os possíveis riscos e benefícios decorrentes de minha participação. Foi-me garantido que posso retirar o meu consentimento a qualquer momento, sem que isto leve a qualquer penalidade.

Tendo em vista os itens acima apresentados, eu, de forma livre e esclarecida, manifesto meu consentimento para participar da pesquisa.

() Aceito Participar da pesquisa

() Não aceito participar da pesquisa

ANEXO C - Cartilha de boas práticas éticas em smartwatches

Como contribuição desta pesquisa para o campo do design, foi desenvolvida uma cartilha para que designers e desenvolvedores possam aplicar no desenvolvimento de soluções para smartwatches a fim de mitigar os problemas e riscos encontrados ao longo deste estudo. As Figuras de E1 a E10 correspondem ao material produzido e disponibilizado no [Google Drive](#).

Figura E1 - Capa da Cartilha



Figura E2 - Informações sobre os autores

AUTORES

Jayne Silva

Bacharel em Design pela Universidade Federal de Pernambuco (UFPE), Pós-graduada em UX Design pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) Mestranda em Design de Artefatos Digitais pela UFPE.

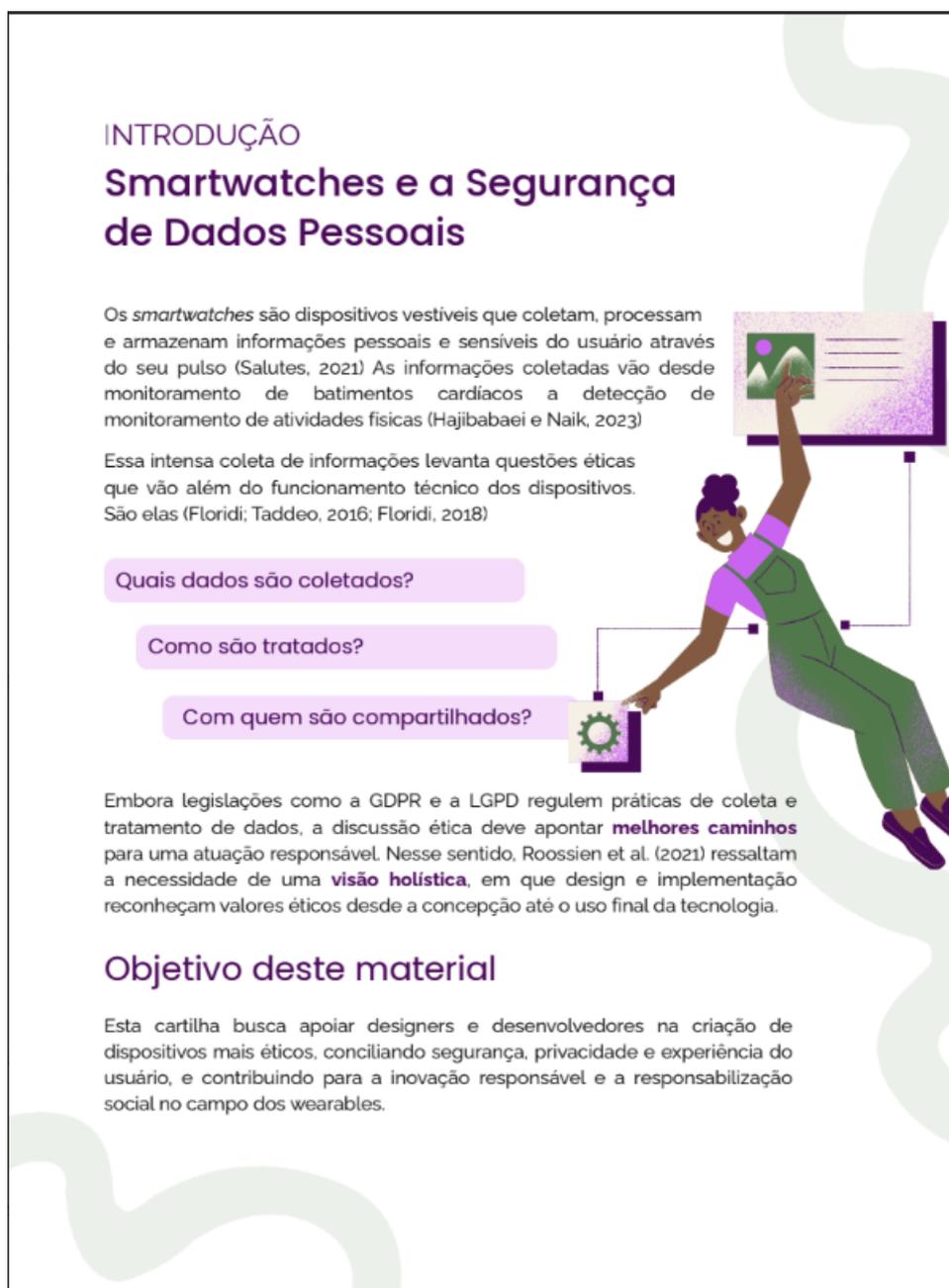
Contato

silvajayne58@gmail.com

João Marcelo Teixeira

Doutor em Ciências da Computação pela Universidade Federal de Pernambuco (UFPE), com período de doutorado sanduiche na Universidade do Chile. Atualmente é Professor Adjunto 3 e chefe do Departamento de Eletrônica e Sistemas da UFPE, além de integrar os colegiados da Pós-graduação em Design e em Engenharia Elétrica. Pesquisa e atua nas áreas de sistemas embarcados, interação humano-computador, dispositivos de interação, realidade virtual e aumentada, computação de alto desempenho e programação paralela. É pesquisador sênior do Voxar Labs (CIn/UFPE).

Figura E3 - Introdução e Objetivo da cartilha



The infographic features a woman in green overalls and a purple shirt interacting with a large screen displaying a mountain landscape. To her left, three purple rounded rectangles contain the questions: 'Quais dados são coletados?', 'Como são tratados?', and 'Com quem são compartilhados?'. Below these, a gear icon is connected to a small device. The background has light green wavy patterns.

INTRODUÇÃO

Smartwatches e a Segurança de Dados Pessoais

Os *smartwatches* são dispositivos vestíveis que coletam, processam e armazenam informações pessoais e sensíveis do usuário através do seu pulso (Salutes, 2021) As informações coletadas vão desde monitoramento de batimentos cardíacos a detecção de monitoramento de atividades físicas (Hajibabaei e Naik, 2023)

Essa intensa coleta de informações levanta questões éticas que vão além do funcionamento técnico dos dispositivos. São elas (Floridi; Taddeo, 2016; Floridi, 2018)

Quais dados são coletados?

Como são tratados?

Com quem são compartilhados?

Embora legislações como a GDPR e a LGPD regulem práticas de coleta e tratamento de dados, a discussão ética deve apontar **melhores caminhos** para uma atuação responsável. Nesse sentido, Roossien et al. (2021) ressaltam a necessidade de uma **visão holística**, em que design e implementação reconheçam valores éticos desde a concepção até o uso final da tecnologia.

Objetivo deste material

Esta cartilha busca apoiar designers e desenvolvedores na criação de dispositivos mais éticos, conciliando segurança, privacidade e experiência do usuário, e contribuindo para a inovação responsável e a responsabilização social no campo dos wearables.

Figura E4 - Principais riscos identificados

Figura E5 - Recomendações para designers e desenvolvedores

Recomendações para designers e desenvolvedores

 **Transparência na coleta e uso de dados**

- Explicar de forma clara e acessível quais dados são coletados, por quê e como serão usados.
- Oferecer avisos contextuais no momento da coleta (ex.: *"Seu batimento cardíaco está sendo compartilhado com aplicativo X"*).

 **Privacidade por padrão (Privacy by Design)**

- Definir como padrão as configurações mais restritivas de compartilhamento.
- Permitir que o usuário personalize facilmente os níveis de coleta de dados.

 **Minimização e retenção de dados**

- Coletar apenas o necessário para a funcionalidade do dispositivo.
- Estabelecer prazos claros e curtos de retenção.
- Fornecer opção de exclusão total dos dados pelo usuário.



Figura E6 - Continuação das recomendações



 **Autenticação e proteção**

- Implementar autenticação multifator para acesso aos dados sensíveis.
- Adotar criptografia em trânsito e em repouso.
- Prever mecanismos contra ataques de replay e replicação de biometria comportamental.

 **Comunicação clara e acessível**

- Adaptar a linguagem conforme o perfil do usuário (considerando escolaridade e faixa etária).
- Usar ícones, infográficos e mensagens simples para explicar riscos e boas práticas.

 **Ética e confiança no design**

- Evitar práticas manipulativas (*deceptive patterns*) que induzam o usuário a compartilhar mais dados.
- Incluir testes de usabilidade focados em compreensão da privacidade.
- Incorporar princípios éticos desde a concepção do produto, e não apenas como complemento final.

Figura E7 - Checklist e conclusão da cartilha

Checklist rápido para o time de design e desenvolvimento

- Dados coletados são estritamente necessários?
- Usuário é informado de forma clara sobre a coleta?
- Existe opção de configurar e excluir dados?
- Há criptografia em todas as etapas do processamento?
- O design foi testado com diferentes perfis de usuários (idade, escolaridade)?
- As práticas adotadas fortalecem a confiança e reduzem riscos éticos?

Conclusão

Projetar *smartwatches* e outros *wearables* de forma ética significa equilibrar **inovação** e **responsabilidade**. Incorporar segurança, privacidade e transparência ao design não apenas protege o usuário, mas também fortalece a confiança na tecnologia e a reputação da marca.



Figura E8 - Referências da cartilha

Referências

CYBERSEC BRAZIL. SmartAttack: nova técnica usa smartwatches para roubar dados de sistemas isolados via sinal ultrassônico. 11 jun. 2025. Disponível em: <https://www.cybersecbrazil.com.br/post/smartattack-nova-t%C3%A9cnica-usa-smartwatches-para-roubar-dados-de-sistemas-isolados-via-sinal-ultrass%C3%B4>. Acesso em: 3 set. 2025.

FAWLE, H.; LEBLANC, D. Smartwatch Vulnerability Analysis: Focusing on Bluetooth Low Energy. IS.I s.n.] 2024.

IFLORIDI, L. Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, v. 376, n. 2133, 28 nov. 2018.

IFLORIDI, L.; TADDEO, M. What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Royal Society of London, 28 dez. 2016.

HAJIBABAEI, N.; NAIK, K. Enhancing Security and Data rates of Smartwatches. 2023.

NASKAR. Data security concerns in wearable devices 2024. Disponível em: <https://www.naskario/>. Acesso em: 3 set. 2025.

OLIVEIRA, Jayne S. Design ético de wearables: investigando a experiência do usuário sobre ética, privacidade e segurança em smartwatches. Dissertação (Mestrado em Design de Artefatos Digitais) – [UFPE], [Recife], em elaboração, 2025.

ROOSIEN, C. C. et al. Ethics in Design and Implementation of Technologies for Workplace Health Promotion: A Call for Discussion. *Frontiers in Digital Health*, v. 3, 20 ago. 2021.

SALUTES, Bruno. Para que servem os sensores de um smartwatch?. IS. U. 26 jul. 2021. Disponível em: <https://canaltech.com.br/smartwatch/para-que-servem-os-sensores-de-um-smartwach/>. Acesso em: 29 out. 2024.



Figura E9 - Contracapa da cartilha

