Mapeamento Sistemático sobre Ética e Segurança em Dispositivos de Internet das Coisas Médicas

Amanda Veras[1], Arthur Callado[2], Cleitianne Oliveira[1], Carina Oliveira[3], Joyce Quintino[1], Joseane Alves[1], Rossana Andrade[1]

[1]Grupo de Redes de Computadores, Engenharia de Software e Sistemas (GREat)
Mestrado e Doutorado em Ciência da Computação (MDCC)
Universidade Federal do Ceará (UFC)

[2]Programa de Pós-Graduação em Computação (PCOMP)
Universidade Federal do Ceará (UFC) - Campus de Quixadá

[3]Programa de Pós-Graduação em Ciência da Computação (PPGCC)
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

acorreiaveras@alu.ufc.com, arthur@ufc.br, cleitianne@alu.ufc.br,
carina@lar.ifce.edu.br, joycequintinoalves@alu.ufc.br,
joseane@alu.ufc.br,rossana@ufc.br

Abstract. *The Internet of Medical Things (IoMT) is revolutionising the healthcare sector by enabling real-time patient monitoring and supporting more accurate diagnoses. However, the increasing use of this technology raises important ethical and security concerns related to the privacy of sensitive data and compliance with regulations. This systematic literature mapping aims to identify the main ethical dilemmas, privacy risks, and recommended technical guidelines to ensure the safe and ethical adoption of IoMT. The analysis was based on papers published between 2019 and 2025, sourced from reputable databases. The results reveal challenges such as algorithmic fairness, informed consent, data control, and the need for more robust regulations to keep pace with the advancement of IoMT.*

Resumo. *A Internet das Coisas Médicas (IoMT) está revolucionando o setor da saúde, possibilitando o monitoramento em tempo real de pacientes e promovendo diagnósticos mais precisos. No entanto, o uso crescente dessa tecnologia levanta importantes questões éticas e de segurança relacionadas à privacidade dos dados sensíveis e à conformidade com regulamentações. Este mapeamento sistemático da literatura tem como objetivo identificar os principais dilemas éticos, riscos à privacidade e diretrizes técnicas recomendadas para garantir a adoção segura e ética da IoMT. A análise foi realizada com base em artigos publicados entre 2019 e 2025, extraídos de bases de dados renomadas. Os resultados revelam desafios como a justiça algorítmica, o consentimento informado, o controle sobre os dados e a necessidade de regulamentações mais robustas para acompanhar o avanço da IoMT.*

1. Introdução

Nos últimos anos, a Internet das Coisas (*Internet of Things* – IoT) tem experimentado uma expansão exponencial em diversos setores, com destaque para a área de saúde, onde

deu origem à Internet das Coisas Médicas (*Internet of Medical Things* - IoMT). Esta tecnologia permite que dispositivos e sensores conectados coletem, transmitam e analisem dados em tempo real, promovendo transformações significativas na prestação de serviços de saúde. A IoMT contribui para diagnósticos mais precisos, tratamentos personalizados e monitoramento contínuo de pacientes, promovendo uma modernização da assistência médica [Shanmugam and Azam 2023].

O mercado global da IoMT tem registrado um crescimento expressivo, com estimativas apontando uma elevação de US$ 72,5 bilhões em 2020 para US$ 188,2 bilhões até 2025 [Shanmugam and Azam 2023]. Tal projeção evidencia a crescente relevância e adoção dessa tecnologia no contexto da saúde mundial.

Entretanto, paralelamente aos benefícios proporcionados pela IoMT, emergem importantes desafios éticos e de segurança que demandam atenção. A coleta e o uso de dados sensíveis dos pacientes suscitam preocupações relacionadas à privacidade, ao consentimento informado, à equidade no acesso aos serviços de saúde digitalizados e à responsabilidade quanto à gestão dessas informações [Qadri et al. 2020]. Nesse contexto, a segurança dos sistemas IoMT torna-se uma preocupação central, uma vez que estão expostos a diversas ameaças cibernéticas capazes de comprometer a integridade dos dados e minar a confiança dos pacientes nos serviços de saúde digital [Messinis et al. 2024].

Dados recentes reforçam a gravidade desse cenário. Nos últimos anos, a adoção massiva de tecnologias conectadas no setor de saúde tem sido acompanhada por um aumento alarmante nas violações de dados sensíveis. Apenas em 2024, mais de 275 milhões de registros de saúde foram expostos, o que corresponde a dados de aproximadamente 82% da população dos Estados Unidos [Alder 2025]. Estima-se que, atualmente, 35% dos ataques cibernéticos tenham como alvo principal o setor da saúde em âmbito global. No Brasil, por exemplo, plataformas do Ministério da Saúde foram alvo de um ataque em 2021, ocasionando a indisponibilidade de serviços, comprometendo os levantamentos estatísticos e inviabilizando a emissão de documentos digitais essenciais [Felix 2023].

A privacidade é a base da confiança de um sistema, sendo um requisito para a aceitação de uma tecnologia pelos usuários [Krontiris et al. 2020]. Estudos indicam que a maioria dos usuários demonstra preocupação significativa com a privacidade de seus dados de saúde ao utilizar dispositivos IoT [Wakili and Bakkali 2024]. Além disso, à medida que as tecnologias IoT passam a integrar de forma crescente a vida cotidiana, torna-se essencial que os marcos legais evoluam para lidar com os desafios éticos e jurídicos emergentes, equilibrando inovação tecnológica com a proteção dos direitos individuais e a segurança pública [Dhinakaran et al. 2025]. Diante desse cenário, torna-se imprescindível a construção de uma base ética e normativa robusta que acompanhe a evolução da IoMT, assegurando sua adoção responsável e a preservação dos princípios fundamentais da assistência à saúde.

Diante desse cenário, este trabalho tem como objetivo realizar um mapeamento sistemático da literatura a fim de identificar os principais dilemas éticos, riscos à privacidade e diretrizes técnicas voltadas à segurança em soluções baseadas em IoMT. As principais contribuições deste estudo incluem: (i) uma categorização estruturada dos desafios éticos e de segurança emergentes na aplicação de tecnologias IoMT; (ii) a síntese das melhores práticas e recomendações técnicas propostas pela literatura recente; e (iii)

a identificação de lacunas de pesquisa e direcionamentos para futuras investigações. Ao sistematizar o conhecimento existente, este trabalho busca apoiar pesquisadores, desenvolvedores e formuladores de políticas na construção de soluções mais éticas, seguras e centradas no usuário no domínio da saúde digital.

2. Trabalhos Relacionados

O estudo de [Zandesh et al. 2019] apresenta uma revisão sistemática da literatura sobre os aspectos legais da computação em nuvem aplicada à área da saúde, com foco na construção de um *framework* legal para ambientes de nuvem na saúde. A revisão mapeou os artigos em cinco categorias centrais: conformidade, proteção de dados, gestão de identidades e credenciais, propriedade dos dados e qualidade de serviço. Embora o artigo forneça uma contribuição relevante, o estudo não contempla a complexidade das tecnologias de IoMT, tampouco aprofunda discussões sobre os dilemas éticos.

O estudo de [Zhang and Navimipour 2022] realiza uma revisão abrangente sobre o papel da IoT na gestão médica inteligente, com foco na integração entre tecnologias, análise de grandes volumes de dados médicos e categoriza essas aplicações em três principais fases: coleta, troca e armazenamento de dados. Os autores destacam os benefícios da IoT na prestação de serviços médicos remotos, melhoria da eficiência, redução de custos e suporte à gestão pública de saúde. No entanto, embora o estudo reconheça a importância da segurança e da privacidade dos dados, sua abordagem é predominantemente orientada à eficiência operacional, com foco limitado nos aspectos éticos e nas implicações sociais mais amplas da adoção dessas tecnologias.

Entre os trabalhos relacionados, destaca-se o estudo de [Wakili and Bakkali 2024], que apresenta uma revisão sistemática da literatura sobre as considerações éticas envolvendo a integração da Internet das Coisas na saúde digital. Este trabalho analisa diversos *frameworks* éticos e identifica os principais desafios enfrentados no uso de tecnologias IoT em ambientes clínicos, com ênfase em questões como privacidade, consentimento, justiça algorítmica, conformidade regulatória, design ético e acesso equitativo aos serviços de saúde. Os autores ressaltam a importância de incorporar considerações éticas desde as fases iniciais de desenvolvimento das soluções em IoT para saúde. Apesar das contribuições dos trabalhos revisados, observa-se a ausência de uma análise integrada que una aspectos éticos, riscos à privacidade e diretrizes técnicas. A Seção 3 apresenta a metodologia adotada neste estudo para suprir essa lacuna.

3. Metodologia

A metodologia utilizada neste trabalho segue as etapas propostas por [Wohlin et al. 2012], conforme ilustrado na Figura 1. Além disso, para assegurar uma análise abrangente sobre ética, privacidade e segurança no contexto da IoMT, foi conduzido um mapeamento sistemático da literatura, fundamentada nos princípios de mapeamento sistemático descritos por [Kitchenham et al. 2009]. O objetivo principal deste mapeamento sistemático é selecionar e reunir informações relevantes sobre o tema proposto. As etapas de planejamento, a estratégia de busca, bem como os critérios de inclusão e exclusão são detalhados ao longo desta seção.

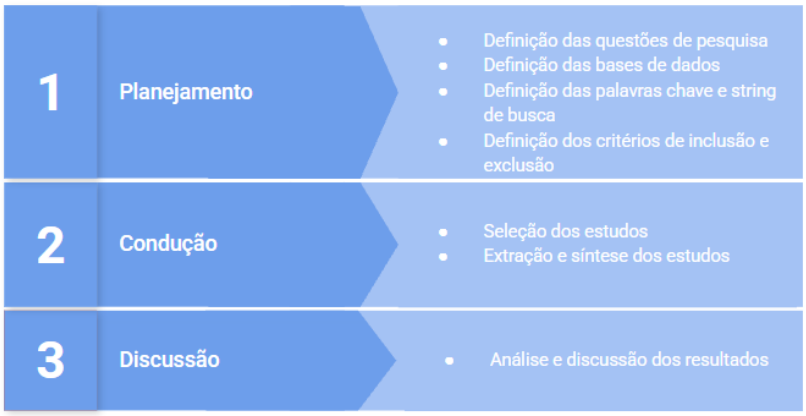

Figura 1. Etapas da metodologia.

3.1. Etapa 1: Planejamento

A etapa de planejamento envolve a definição das bases conceituais do mapeamento, abrangendo a formulação das questões de pesquisa, a escolha das bases de dados, a seleção das palavras-chave, a construção da *string* de busca e o estabelecimento dos critérios de inclusão e exclusão. Essa fase é fundamental para assegurar a objetividade e a reprodutibilidade de todo o processo do mapeamento.

3.1.1. Definição das Questões de Pesquisa

Três Questões de Pesquisa (QP) foram definidas para o mapeamento da literatura. As respostas dessas questões permitem conhecer o estado da arte sobre ética e segurança em dispositivos da Internet das Coisas Médicas. As questões de pesquisas estão detalhadas na Tabela 1.

No.	Questão de Pesquisa
QP1	Quais são os principais dilemas éticos envolvidos no desenvolvimento e uso de tecnologias de IoMT?
QP2	Quais são os principais riscos à privacidade em ambientes IoMT, e como esses riscos afetam a segurança e a confiança dos usuários no uso de dispositivos de saúde conectados?
QP3	Quais boas práticas, diretrizes técnicas e políticas regulatórias têm sido recomendadas para garantir a privacidade e a conformidade ética em soluções baseadas em IoMT?

Tabela 1. Questões de Pesquisa do Mapeamento Sistemático da Literatura.

3.1.2. Definição das bases de dados

A escolha de bases de dados confiáveis e amplamente reconhecidas é essencial para assegurar a relevância e a qualidade dos estudos selecionados. Para este mapeamento, foram

utilizadas quatro fontes amplamente adotadas na literatura científica: IEEE Xplore[1], ACM Digital Library[2], ScienceDirect [3] e Scopus[4].

3.1.3. Definição das palavras chave e *string* de busca

A elaboração da estratégia de busca é um passo crucial para garantir a recuperação de estudos relevantes. Neste trabalho, foram definidas palavras-chave relacionadas aos principais conceitos abordados na pesquisa, com o objetivo de alcançar uma cobertura abrangente da literatura. A *string* de busca utilizada foi:

(“internet of health things” OR “internet of things”) AND (“security”OR “privacy”) AND (“data protection”) AND (“ethics”)

3.1.4. Definição dos critérios de inclusão e de exclusão

Para assegurar a qualidade e a pertinência dos estudos analisados, foram estabelecidos critérios claros de inclusão e exclusão. Esses critérios orientaram a triagem dos resultados obtidos nas bases de dados, conforme detalhado na Tabela 2.

Critérios	
Inclusão	Estudos publicados entre 2019 e 2025.
	Artigos publicados em inglês.
	Artigos revisados por pares e trabalhos apresentados em conferências.
	Pesquisas com foco em Internet das Coisas Médicas (IoMT) ou Internet das Coisas (IoT).
	Estudos que abordem considerações éticas em IoT.
	Pesquisas que discutem proteção de dados, privacidade ou questões de segurança em IoT.
Exclusão	Estudos inacessíveis ou cujo texto completo não estejam disponíveis.
	Artigos em idiomas diferentes do inglês.
	Estudos secundários.
	Artigos publicados antes de 2019.

Tabela 2. Critérios de inclusão e exclusão.

3.2. Etapa 2: Condução

A condução do mapeamento sistemático consiste na aplicação prática da estratégia de busca, coleta de artigos, análise de títulos e resumos, leitura completa dos textos e extração das informações relevantes. Essa etapa visa garantir a seleção rigorosa dos estudos que respondam às questões de pesquisa.

[1]https://ieeexplore.ieee.org/
[2]https://dl.acm.org/
[3]https://www.sciencedirect.com/
[4]https://www.scopus.com/

3.2.1. Seleção dos estudos

A seleção foi conduzida em duas fases. Na primeira, foram analisados títulos, resumos e palavras-chave. Na segunda, foi feita a leitura completa dos artigos potencialmente relevantes. Apenas os estudos que atenderam aos critérios de inclusão foram mantidos para análise posterior.

3.2.2. Extração e síntese dos estudos

A extração dos dados consistiu no preenchimento de uma ficha padronizada contendo informações tais como: ano de publicação, autores, objetivos, abordagem metodológica, aspectos éticos discutidos, riscos de privacidade identificados e recomendações apresentadas.

Os dados extraídos foram organizados em categorias temáticas que permitiram uma análise qualitativa dos estudos. A síntese envolveu a identificação de padrões recorrentes, lacunas na literatura e tendências em relação ao uso ético e seguro de dispositivos IoMT.

3.3. Etapa 3: Discussão

Esta etapa compreende a interpretação dos resultados obtidos no mapeamento, respondendo às QP com base nas evidências coletadas. Também são discutidas as limitações do estudo e sugestões para pesquisas futuras.

3.3.1. Análise e discussão dos resultados

Os resultados foram analisados de forma qualitativa, buscando responder diretamente às questões de pesquisa e destacar as abordagens mais frequentes nos estudos. Os aspectos identificados foram organizados por frequência e relevância temática.

Um total de 1.192 artigos foram inicialmente identificados nas bases de dados digitais, conforme apresentado na Tabela 3. Após a aplicação dos critérios de inclusão e exclusão previamente definidos, foram eliminados os estudos que não atendiam aos requisitos metodológicos ou de escopo da pesquisa. Além disso, os artigos remanescentes foram avaliados quanto à sua relevância em relação às perguntas e objetivos desta pesquisa. O conjunto final de estudos selecionados, considerados adequados para análise, encontra-se detalhado na Tabela 3.

Base de dados	Artigos encontrados	Artigos aceitos
IEEE Xplore	44	24
ACM Digital Library	530	29
ScienceDirect	600	125
Scopus	18	5

Tabela 3. Distribuição dos artigos encontrados e aceitos por base de dados.

A análise dos 183 artigos selecionados forneceu uma visão abrangente dos principais desafios éticos e de privacidade associados ao uso de tecnologias de saúde baseadas

em dados. Os resultados foram organizados em categorias temáticas recorrentes na literatura, as quais são apresentadas e detalhadas na Seção 4, com o objetivo de oferecer uma compreensão estruturada dos aspectos críticos identificados.

4. Resultados

Esta seção apresenta as respostas às questões de pesquisa delineadas na Seção 3.1.1, organizadas em subseções correspondentes.

A literatura identifica alguns dilemas relacionados ao desenvolvimento e à aplicação de tecnologias da IoMT, os quais envolvem aspectos como privacidade, justiça, transparência, autonomia e responsabilidade.

4.1. QP1: Quais são os principais dilemas éticos envolvidos no desenvolvimento e uso de tecnologias de IoMT?

Um dos primeiros desafios destacados refere-se à privacidade mental, à autonomia da tomada de decisões e à identidade pessoal associados ao uso de tecnologias de *Brain Computer Interface* (BCI)[5]. Essas tecnologias, ao permitirem a comunicação direta entre o cérebro humano e dispositivos externos, afetam diretamente a subjetividade humana. Nesse contexto, torna-se imprescindível o desenvolvimento de *frameworks* regulatórios que assegurem o controle rigoroso dos dados coletados e estabeleçam responsabilidades claras pelas ações mediadas por essas interfaces, garantindo justiça, transparência e segurança em sistemas sociotécnicos [Botes 2022].

Outro dilema ético recorrente diz respeito à igualdade no acesso às tecnologias. Dispositivos destinados à ampliação cognitiva, por exemplo, podem ampliar desigualdades sociais preexistentes, especialmente quando o acesso a tais tecnologias é restrito por barreiras econômicas, limitando seus benefícios [Botes 2022].

No âmbito de casas inteligentes, surgem questões relacionadas à privacidade e aos desequilíbrios de poder entre usuários primários (como proprietários) e não primários (como inquilinos, crianças ou trabalhadores). Frequentemente, esses últimos não possuem controle nem conhecimento sobre os dados coletados, o que pode implicar em vigilância e na redução da autonomia desses grupos. Embora a vigilância possa ter funções protetivas, ela também pode reforçar assimetrias de poder. Para reduzir tais impactos, pesquisadores sugerem que os sistemas sejam projetados de forma flexível, envolvendo tanto usuários primários quanto não primários no processo de concepção e desenvolvimento, a fim de promover maior justiça e inclusão [Wong et al. 2023].

Os algoritmos empregados em processo de tomada de decisão e análise de dados apresentam o risco de reforçar preconceitos e desigualdades sociais, uma vez que são geralmente treinados com grandes volumes de dados que refletem vieses da sociedade. No contexto da saúde, esse problema pode resultar em tratamentos discriminatórios ou ineficazes para determinadas comunidades, grupos étnicos ou gêneros. Para mitigar tais distorções, torna-se imprescindível a realização de auditorias extensivas nos conjuntos de dados utilizados no treinamento dos modelos, com o objetivo de identificar e corrigir possíveis vieses [Saxena et al. 2023].

[5]Interface Cérebro-Computador

O uso de perfilamento automatizado também representa um dilema ético relevante. Essa prática consiste na utilização de dados para fazer inferências sobre indivíduos, frequentemente com o objetivo de prever comportamentos, preferências ou características. Na IoT, essa prática frequentemente envolve decisões automatizadas, que podem levar à discriminação, sobretudo quando as inferências realizadas são imprecisas, baseadas em suposições inadequadas ou baseadas em dados históricos com vieses. Esse fenômeno pode dar origem a ciclos de retroalimentação, nos quais erros iniciais, decorrentes de dados incorretos ou incompletos, são amplificados ao longo do tempo. Por exemplo, uma vigilância mais intensa em determinadas regiões pode aumentar o volume de dados sobre esses locais, gerando perfis de risco que alimentam decisões futuras e intensificam a estigmatização e a exclusão social [Saxena et al. 2023].

A atribuição de responsabilidade diante de falhas ou danos causados por dispositivos conectados configura outro dilema central. A crescente integração da Inteligência Artificial (IA) em sistemas de saúde baseados em IoT tem modificado o papel dos profissionais da área, na medida em que decisões automatizadas reduzem a intervenção humana direta. Esse cenário levanta preocupações quanto à responsabilização por erros ou consequências imprevistas decorrentes do uso dessas tecnologias [Saxena et al. 2023].

Essa problemática estende-se a diversos contextos, como veículos autônomos, casas inteligentes e sistemas de saúde conectados, exigindo uma discussão ética e jurídica sobre a delimitação de responsabilidades entre fabricantes, desenvolvedores, profissionais da saúde, usuários finais e, eventualmente, os próprios sistemas autônomos [Krontiris et al. 2020]. Nesse cenário, é indispensável o estabelecimento de estruturas normativas claras de responsabilização que definam de maneira precisa os papéis e deveres de cada parte interessada. Profissionais da saúde, por exemplo, devem ser capacitados para utilizar essas tecnologias de forma crítica e ética, enquanto os desenvolvedores devem projetar soluções transparentes, auditáveis e assumir a responsabilidade por falhas ou vieses sistêmicos [Saxena et al. 2023].

4.2. QP2: Quais são os principais riscos à privacidade em ambientes IoMT, e como esses riscos afetam a segurança e a confiança dos usuários no uso de dispositivos de saúde conectados?

O avanço das tecnologias de conexão do cérebro humano à internet por meio das BCIs representa um progresso promissor, porém surgem preocupações relacionadas à privacidade e à segurança dos usuários. Um dos principais riscos diz respeito à exposição do cérebro a ataques cibernéticos, pois, caso comprometidos, esses dispositivos podem ficar vulneráveis à extração de informações sensíveis, de modo que afeta a integridade mental dos usuários [Botes 2022].

Esse cenário evidencia a necessidade de se estabelecer marcos regulatórios que acompanhem a evolução das neurotecnologias e assegurem a proteção dos direitos fundamentais [Botes 2022].

A governança de dados de saúde gerados por pacientes (*Patient-Generated Health Data* – PGHD), coletados por dispositivos vestíveis e aplicativos móveis, enfrenta desafios significativos devido a lacunas e sobreposições regulatórias. Nos Estados Unidos, enquanto dados sob a HIPAA — lei federal que regula o uso e a proteção de informações de saúde pessoais — contam com proteções específicas, sua transferência para plataformas

de grandes empresas de tecnologia os submete a políticas comerciais pouco transparentes. Essa ambiguidade normativa compromete a confiança de usuários e profissionais, e abre espaço para práticas de monetização de dados. Além disso, o uso intensivo de IA e ML agrava os riscos de reidentificação, tornando ineficazes os modelos tradicionais de anonimização [Winter and Davidson 2022].

O consentimento do usuário é um requisito legal e ético nos sistemas de IoT em saúde, mas obter um consentimento verdadeiramente informado é um desafio significativo nesse contexto. A obtenção do consentimento em ambientes IoT é complexa devido à diversidade de dispositivos, à coleta automatizada de dados e à limitada compreensão dos usuários sobre privacidade digital. Em ambientes IoMT, os principais riscos associados ao consentimento incluem a coleta não transparente de dados por sensores, o uso secundário não autorizado das informações, a ausência de mecanismos para revogação do consentimento e a possibilidade de reidentificação de dados previamente anonimizados [Velmovitsky et al. 2020]. Tais fatores comprometem a autodeterminação informacional[6] dos usuários e enfraquecem a confiança nas tecnologias de saúde conectadas.

4.3. QP3: Quais boas práticas, diretrizes técnicas e políticas regulatórias têm sido recomendadas para garantir a privacidade e a conformidade ética em soluções baseadas em IoMT?

Torna-se urgente repensar os direitos fundamentais diante da crescente integração entre seres humanos e tecnologia, visando um novo modelo de governança constitucional que oriente o desenvolvimento ético, justo e seguro dessas tecnologias emergentes [Botes 2022].

Autores como [Chhetri and Genaro Motti 2022] destacam a necessidade de regulamentação governamental e certificações de terceiros para garantir a proteção dos dados. Considerando que os usuários frequentemente não possuem conhecimento ou capacidade para gerenciar configurações complexas de privacidade, a proteção deve ser incorporada desde o início por meio de estratégias de design que limitem a coleta de dados e priorizem a segurança dos usuários.

Os autores de [Chalhoub et al. 2021] propõem recomendações de design, como o aprimoramento da experiência do consentimento, considerando a sua revogação, alterações ao longo do tempo e erros cometidos pelos usuários. Assim como a identificação e uma comunicação clara dos riscos associados a funcionalidades sensíveis, como câmeras e assistentes virtuais. Além disso, recomenda-se o investimento em controles tangíveis de privacidade, como desligamentos físicos ou indicadores visíveis, que proporcionam maior sensação de segurança do que políticas abstratas de uso de dados.

Para garantir um consentimento informado em sistemas de saúde baseados em IoT, [Velmovitsky et al. 2020] propõem diretrizes centradas no usuário, com foco em linguagem acessível, recursos visuais e mecanismos de revogação de consentimento. A proposta inclui elementos como vídeos explicativos, testes de compreensão, apresentação contextualizada da política de privacidade e suporte a consentimento dinâmico. Essas práticas buscam facilitar a compreensão, promover transparência e fortalecer a autodeterminação informacional dos usuários em conformidade com regulamentações como o GDPR.

[6]https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

O uso de *blockchain* pode proporcionar armazenamento seguro dos grandes volumes de dados coletados por sensores e dispositivos de IoT, organizando-os em blocos. Usuários ou dispositivos autorizados podem autenticar e identificar outros nós sem depender de autoridades certificadoras terceirizadas. Além disso, a natureza distribuída do *blockchain* elimina o risco de um ponto único de falha em sistemas de IoT [Siddiqua Oosman and Dudhe 2021].

Estudos na área médica enfrentam desafios relacionados ao armazenamento de dados, aprovações éticas e regulamentações, como o Art. 5o da *General Data Protection Regulation* (GDPR)[7], que impõe restrições de uso e finalidade dos dados. A medicina personalizada, baseada em agrupamento de pacientes, exige conformidade com esses requisitos. O aprendizado federado (*Federated Learning* - FL) surge como solução ao permitir treinar modelos de aprendizado de máquina (*Machine Learning* - ML) de forma colaborativa sem compartilhar dados brutos, utilizando uma arquitetura cliente-servidor para agregar parâmetros. Na área da saúde, tais modelos devem ser altamente seguros e confiáveis, visto que falhas podem ser fatais. Dessa forma, é essencial proteger sistemas FL contra ataques, como envenenamento de modelos, antes de sua implementação em ambientes hospitalares [Pfitzner et al. 2021].

O trabalho [Rehman et al. 2022] propõe a integração do FL com *blockchain* para aprimorar os sistemas de Saúde 5.0, com foco na IoMT. O FL permite o treinamento descentralizado de modelos de aprendizado de máquina entre dispositivos de borda e organizações médicas, preservando a privacidade dos dados dos pacientes. Ao combinar criptografia avançada com *blockchain*, o estudo aborda questões de segurança, incluindo a proteção da privacidade e a integridade dos dados.

5. Conclusão

A IoMT tem demonstrado grande potencial para transformar o setor de saúde, oferecendo avanços significativos em diagnóstico, tratamento e monitoramento de pacientes. No entanto, o crescimento dessa tecnologia está acompanhado de desafios éticos e de segurança que não podem ser negligenciados.

Com base nos artigos selecionados, este estudo respondeu às três questões de pesquisa propostas. Em relação à QP1, foram identificados dilemas éticos como a privacidade mental em interfaces cérebro-computador, a desigualdade no acesso às tecnologias, o uso de perfilamento automatizado e a responsabilidade em falhas de sistemas. Quanto à QP2, observou-se que os principais riscos à privacidade incluem a exposição a ataques cibernéticos, a reidentificação em dados anonimizados e a ausência de controle granular por parte dos usuários sobre seus dados. Em resposta à QP3, a literatura aponta a necessidade de políticas regulatórias mais robustas, uso de blockchain para segurança descentralizada, aprendizado federado para preservação da privacidade e design centrado no usuário com mecanismos de consentimento revogável.

Essas evidências reforçam a necessidade de um arcabouço ético, técnico e legal sólido que acompanhe o avanço da IoMT. Dessa forma, será possível consolidar essa tecnologia como uma ferramenta eficaz, segura e justa para a saúde digital do futuro.

[7]https://gdpr-info.eu/art-5-gdpr/

Referências

Alder, S. (2025). 2024 healthcare data breach report. Disponível em: https://www.hipaajournal.com/2024-healthcare-data-breach-report/. Acessado em 19 jul. 2025.

Botes, M. W. M. (2022). Brain computer interfaces and human rights: Brave new rights for a brave new world. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '22, page 1154–1161, New York, NY, USA. Association for Computing Machinery.

Chalhoub, G., Kraemer, M. J., Nthala, N., and Flechais, I. (2021). "it did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA. Association for Computing Machinery.

Chhetri, C. and Genaro Motti, V. (2022). User-centric privacy controls for smart homes. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2).

Dhinakaran, D., Raja, S. E., Ramathilagam, A., Vennila, G., and Alagulakshmi, A. (2025). Ethical and legal challenges with iot in home digital twins. *ICT Express*.

Felix, P. (2023). Setor de saúde tem epidemia de hackers – e brasil é um dos mais expostos. Disponível em: https://veja.abril.com.br/saude/setor-de-saude-tem-epidemia-de-hackers-e-brasil-e-um-dos/mais-expostos. Acesso em: 22/04/2024.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering – a systematic literature review. *Information and Software Technology*, 51(1):7–15.

Krontiris, I., Grammenou, K., Terzidou, K., Zacharopoulou, M., Tsikintikou, M., Baladima, F., Sakellari, C., and Kaouras, K. (2020). Autonomous vehicles: Data protection and ethical considerations. In *Proceedings of the 4th ACM Computer Science in Cars Symposium*, CSCS '20, New York, NY, USA. Association for Computing Machinery.

Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., and Doulamis, N. (2024). Enhancing internet of medical things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, page 108036.

Pfitzner, B., Steckhan, N., and Arnrich, B. (2021). Federated learning in a medical context: A systematic literature review. *ACM Trans. Internet Technol.*, 21(2).

Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., and Kim, S. W. (2020). The future of healthcare internet of things: A survey of emerging technologies. *IEEE Communications Surveys Tutorials*, 22(2):1121–1167.

Rehman, A., Abbas, S., Khan, M., Ghazal, T. M., Adnan, K. M., and Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine*, 150:106019.

Saxena, R., Sharma, V., and Gupta, M. (2023). Ethical and social consequences of computer vision and ai-integrated iot technologies in the medical ecosystem. In *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, pages 1018–1023.

Shanmugam, B. and Azam, S. (2023). Risk assessment of heterogeneous iomt devices: A review. *Technologies*, 11(1):31.

Siddiqua Oosman, B. and Dudhe, R. (2021). Review on the ethical and legal challenges with iot. In *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, pages 529–534.

Velmovitsky, P. E., Miranda, P. A. D. S. E. S., Vaillancourt, H., Donovska, T., Teague, J., and Morita, P. P. (2020). A blockchain-based consent platform for active assisted living: Modeling study and conceptual framework. *Journal of Medical Internet Research*, 22(12).

Wakili, A. and Bakkali, S. (2024). Internet of things in healthcare: An adaptive ethical framework for iot in digital health. *Clinical eHealth*, 7:92–105.

Winter, J. S. and Davidson, E. (2022). Harmonizing regulatory regimes for the governance of patient-generated health data. *Telecommunications Policy*, 46(5):102285.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media.

Wong, R. Y., Valdez, J. C., Alexander, A., Chiang, A., Quesada, O., and Pierce, J. (2023). Broadening privacy and surveillance: Eliciting interconnected values with a scenarios workbook on smart home cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, DIS '23, page 1093–1113, New York, NY, USA. Association for Computing Machinery.

Zandesh, Z., Ghazisaeedi, M., Devarakonda, M. V., and Haghighi, M. S. (2019). Legal framework for health cloud: A systematic review. *International Journal of Medical Informatics*, 132:103953.

Zhang, G. and Navimipour, N. J. (2022). A comprehensive and systematic review of the iot-based medical management systems: Applications, techniques, trends and open issues. *Sustainable Cities and Society*, 82:103914.