REVISTA
DESAFIOS
ISSN: 2359-3652

V.11, n.8, 2024 – *DOI:* http://dx.doi.org/10.20873/DGGP_2024_11_10

PROTEÇÃO E PRIVACIDADE DOS DADOS EM SAÚDE: OS DESAFIOS EM DISPOSITIVOS INTELIGENTES DISPONIBILIZADOS PELA INTERNET DAS COISAS (IOT)

PROTECTION AND PRIVACY OF HEALTH DATA: THE CHALLENGES IN SMART DEVICES AVAILABLE ON THE INTERNET OF THINGS (IOT)

PROTECCIÓN Y PRIVACIDAD DE LOS DATOS DE SALUD: LOS DESAFÍOS EN LOS DISPOSITIVOS INTELIGENTES DISPONIBLES POR INTERNET DE LAS COSAS (IDC)

MARA LUCIA DOS SANTOS COSTA:

Doutoranda em Modelagem Computacional de Sistemas pelo Programa de Pós-Graduação em Modelagem Computacional de Sistemas. Universidade Federal do Tocantins (UFT). E-mail: mara.costa1@mail.uft.edu.br | Orcid.org/ 0009-0000-2284-291X

MARIANE MORAES:

Programa de Pós-Graduação em Modelagem Computacional de Sistemas, Universidade Federal do Tocantis. Universidade Federal do Tocantins (UFT). E-mail: moraes.mariane@gmail.com | Orcid.org/0000-0002-3323-7712

GENTIL VELOSO BARBOSA:

Professor do Departamento de Ciência da Computação. Universidade Federal do Tocantins (UFT). E-mail: gentil@uft.edu.br | Orcid.org/0000-0001-5622-516X

DAVID NADLER PRATA:

Professor do Departamento de Ciência da Computação. Universidade Federal do Tocantins (UFT). E-mail: ddnprata@gmail.com | Orcid.org/0000-0002-1414-4000

HUMBERTO XAVIER DE ARAUJO:

Professor do Departamento de Engenharia Elétrica. Universidade Federal do Tocantins (UFT). E-mail: hxaraujo@mail.uft.edu.br | Orcid.org/0000-0002-3321-4166

Artigo recebido: 23/09/2023 Aceito em: 07/11/2024 Publicado em: 20/12/2024

Como citar este artigo:

COSTA, Mara Lucia dos Santos.; MORAES, Mariane.; BARBOSA, G. V.; PRATA, D. N.; ARAUJO, H. X. Proteção e Privacidade dos Dados em Saúde: Os Desafios em Dispositivos Inteligentes Disponibilizados pela Internet das Coisas (IOT). **Desafios. Revista Interdisciplinar da Universidade Federal do Tocantins**. Palmas, v. 11, n. 8, 2024. DOI: http://dx.doi.org/10.20873/DGGP_2024_11_11

REVISTA DESAFIOS ISSN: 2359-3652

RESUMO:

A Internet das Coisas (IoT) traz novas perspectivas de cuidado e melhoria da qualidade de vida das pessoas, entretanto, é crescente a preocupação com o sigilo dos dados que trafegam na Internet a partir dos dispositivos de rede sem fio. O artigo tem o objetivo de sistematizar como a comunidade acadêmica está abordando a privacidade dos dados coletados, armazenados e compartilhados por dispositivos habilitados para IoT. Realizada uma revisão integrativa entre 2016 e 2021 com busca na base de dados PubMED. Foram incluídos 45 artigos na revisão final, que mostraram oportunidades para garantir a privacidade dos dados usando, principalmente, criptografia e a tecnologia Blockchain. Com avanço da Pandemia de COVID-19, cada vez mais esses dispositivos ganham magnitude e se faz necessária a governança para definir as responsabilidades e os processos para a captura, tratamento e disponibilização dos dados de saúde, tendo o usuário como protagonista de todo o processo de controle de acesso.

PALAVRAS-CHAVE: Internet das Coisas; Dados em Saúde; Privacidade.

V.11, n.8, 2024. ISSN n° 2359-3652

ABSTRACT:

The Internet of Things (IoT) brings new perspectives to care and improve people's quality of life, however, there is a growing concern about the confidentiality of data that travels on the internet from wireless network devices. The article aims to systematize how the community is approaching the privacy of data collected, stored and shared by IoT-enabled devices. An integrative review was carried out between 2016 and 2021 with a search in the PubMED database. Forty-five articles were mainly cryptography and Blockchain technology. With the advancement of the COVID-19 Pandemic, these devices increasingly gain magnitude and governance is necessary to define responsibilities and processes for capturing, processing and making available health data, with the user as the protagonist of the entire process of access control.

KEYWORDS: *Internet of Things; Health Data; Privacy.*

RESUMEN:

El Internet de las Cosas (IdC) trae nuevas perspectivas de atención y mejora de la calidad de vida de las personas, sin embargo, existe una creciente preocupación por la confidencialidad de los datos que viajan por Internet desde los dispositivos de redes inalámbricas. El artículo tiene como objetivo sistematizar cómo la comunidad académica aborda la privacidad de los datos recopilados, almacenados y compartidos por dispositivos habilitados para IdC. Se realizó una revisión integradora entre 2016 y 2021 mediante búsqueda en la base de datos PubMED. Se incluyeron 45 artículos en la revisión final, que mostró oportunidades para garantizar la privacidad de los datos utilizando principalmente criptografía y tecnología Blockchain. Con el avance de la Pandemia del COVID-19, estos dispositivos ganan cada vez más magnitud y la gobernanza es necesaria para definir responsabilidades y procesos de captura, procesamiento y puesta a disposición de los datos de salud, con el usuario como protagonista de todo el proceso de control de acceso.

PALABRAS CLAVE: *Internet de las Cosas; Datos de Salud; Privacidad.*

INTRODUÇÃO

O desenvolvimento tecnológico da sociedade potencializou o surgimento de novas tecnologias que podem simplificar o dia a dia e proporcionar serviços ou processos produtivos mais eficientes, como as tecnologias baseadas na Internet das Coisas - IoT (Nižetić et al., 2020), que se caracteriza como uma rede de objetos conectados entre si e na Internet, tendo potencial para melhorar a prestação de serviços de saúde. Essas tecnologias trazem uma nova perspectiva para aplicação na área da saúde, por meio de sistemas inteligentes melhorando a saúde e a qualidade de vida da sociedade (Verdejo e Espinosa et al., 2021).

A IoT está cada vez mais sendo incorporada no desenvolvimento de atividades em saúde, sendo usada para monitoramento, diagnóstico e tratamento remoto de pacientes (Monteith et al., 2021). Contudo, o volume de dados produzidos pelos dispositivos médicos baseados em IoT, principalmente dados pessoais, tem aumentado em armazenamento, processamento, tratamento e compartilhamento de diferentes formas entre os provedores de saúde públicos e privados, como hospitais, seguradoras, pagadores e pesquisadores (Dash, 2020).

Para ampla adoção da IoT em saúde é necessário mitigar os riscos cibernéticos, demonstrando que quanto maior o nível de autonomia através do uso da inteligência das coisas, os desafios para proteção das identidades e da privacidade dos pacientes se torna maior, entretanto, possível e adequado (Kelly et al., 2020). Outro desafio é garantir a segurança cibernética adequada devido aos potenciais ataques, que podem ocorrer dentro de sistemas de monitoramento de saúde.

Por isso, os autores John et al., 2019 consideram fundamental observar as implicações de privacidade e segurança dos dados de saúde diante do uso dos dispositivos IoT. Ainda de acordo com os autores YIN et al., 2019, apesar da saúde moderna estar remodelando a presença e a evolução da IoT, que suporta tecnologia, economia e redes sociais, é notório que a privacidade e a proteção de dados precisam de mais atenção, tendo em vista que qualquer uso indevido pode levar uma potencial ameaça.

Nesse mesmo sentido, pesquisadores mostram que a governança das tecnologias de informação e comunicação (TIC) entraram na agenda das organizações em todo o mundo, em decorrência principalmente da pandemia de COVID-19, e reforça a importância do uso da governança das tecnologias na implementação de IOT para aumentar a taxa de sucesso e eficiência nas organizações e serviços (Henriques et al., 2020).

O presente trabalho tem como objetivo sistematizar como a comunidade acadêmica está abordando a privacidade dos dados coletados, armazenados e compartilhados por dispositivos habilitados para Internet das Coisas. Espera-se

V.11, n.8, 2024. ISSN n° 2359-3652

que a reflexão apresentada neste artigo aponte direções de pesquisa para as técnicas e mecanismos necessários no sentido de preservação da privacidade de dados em saúde e governança dos dados, considerando os aspectos e limitações dos dispositivos IoT.

MATERIAIS E MÉTODOS

Este trabalho foi desenvolvido por meio de uma revisão integrativa. A seleção dos artigos foi realizada de maneira ampla tendo em vista que as temáticas de privacidade e segurança aparecem interligadas nas discussões da literatura. Embora haja relação entre as temáticas, neste artigo será abordado a privacidade dos dados para dispositivos IoT. Para nortear essa pesquisa, foi elaborada a seguinte pergunta: Como estão sendo tratadas as questões referentes à privacidade de dados nos dispositivos médicos habilitados para IoT?

Utilizou-se, inicialmente, para a ampla seleção de artigos adotando os seguintes Descritores em Ciências da Saúde (DeCS): “Internet of things”, “health”, “Privacy”, “Security”. Os descritores foram aplicados no título e no corpo do texto para indicar o conteúdo e facilitar sua recuperação. As combinações (“Internet of things” OR “IoT”) AND “health” AND (“Privacy” OR “Security”) foram utilizadas para a pesquisa.

Para selecionar os artigos, a busca bibliográfica ocorreu na base de dados Portal da U.S. National Library of Medicine (PUBMED). Os critérios de inclusão dos artigos, nesta etapa, foram: artigos na íntegra; originais dentro do escopo e temática; documentos oficiais; artigos no idioma inglês revisados por pares e; publicações entre janeiro de 2016 e junho de 2021. Como critério de exclusão dos artigos, não foram considerados artigos repetidos, monografias, dissertações, teses e artigos que tratam de dispositivos fora da área da saúde.

Com o propósito de consolidar a busca, foi elaborado um mapa de busca contendo os DeCS, total de artigos, total de exclusão e total de selecionados. Foram identificados os artigos duplicados e selecionados os artigos após a leitura do título e resumo. Os dados do estudo foram coletados e gerenciados usando as ferramentas eletrônicas de captura de dados REDCap - Research Electronic Data Capture (Harris et al., 2009) (Harris et al., 2019), hospedada na Universidade Federal de Tocantins - UFT. Os campos ano, tipo de publicação, periódico de publicação, autores, título, objetivo, resumo e localização da publicação compuseram a coleta dos dados.

A busca ampla retornou 221 artigos completos com as strings de busca apresentadas anteriormente. Do total de artigos, não foram encontrados duplicidade. Foram excluídos 108 artigos após leitura de título e resumo por não contemplarem a pergunta da pesquisa. Cento e treze artigos foram selecionados para leitura completa. Após leitura, foram excluídos 68 artigos, restando 45

artigos a serem incluídos na revisão, que abordavam o tema de Privacidade ou Privacidade e Segurança conjugados. Ademais, nesse cenário, buscou-se identificar o conjunto de procedimentos e mecanismos de governança no contexto da IoT.

RESULTADOS E DISCUSSÃO

A tabela (Tab. 1) apresenta a distribuição das publicações ao longo do período estudado. Observa-se que as publicações tiveram um crescimento ao longo dos anos a partir do ano 2018. Cabe ressaltar que o ano de 2021 não está representado por completo, uma vez que o mês de corte foi junho.

Tabela 1: Distribuição dos artigos por ano.

ANO	FA (n)	FR (%)
2017	1	2,2
2018	5	11,1
2019	10	22,2
2020	18	40,0
2021	11	24,4
TOTAL	45	100,0

Fonte: Elaborado pelos autores (2023)

A figura (Fig. 1) representa as principais palavras no título dos artigos que possibilitaram a busca da temática sobre privacidade.

Figura 1: Nuvem de palavras dos títulos dos artigos sobre privacidade de dados

Fonte: Elaborado pelos autores (2023)

V.11, n.8, 2024. ISSN n° 2359-3652

Privacidade de dados em dispositivos IoT na área de saúde

A IoT incorpora vários tipos de hardware, protocolos de comunicação e serviços (Mrabet et al., 2020) (Ahad et al., 2020) (Segarra et al., 2020). Ao mesmo tempo que essa diversidade da IoT oferece conforto aos usuários, também pode levar a um grande número de ameaças e ataques à segurança e privacidade (Gope et al., 2021; Laplante et al., 2018; Schukat et al., 2016). A preocupação com privacidade dos dados é necessária e constante (Martín-ruíz et al., 2018) (Dey et al., 2018) (El-hajj et al., 2019).

Segundo Kelly e colaboradores, a temática é vista como uma barreira para a Internet das Coisas (Kelly et al., 2020). A IoT pode possibilitar oportunidades para ataques cibernéticos e para que dados pessoais sejam coletados de forma inadequada (Hussain et al., 2021). Os aplicativos baseados em IoT são vulneráveis a ataques cibernéticos por dois motivos básicos: (1) a maioria das comunicações é sem fio, o que torna a escuta secreta muito fácil; e (2) a maioria dos componentes da IoT são caracterizados por baixa energia e, portanto, dificilmente podem implementar esquemas complexos por conta própria para garantir a segurança. Como os dados de saúde muitas vezes contêm informações pessoais e confidenciais, os sistemas de saúde devem fornecer um esquema de autenticação de usuário seguro (Ryu et al., 2020).

Por meio do estudo de Ismail (Ismail et al., 2020) é possível constatar que os sistemas de gerenciamento de dados de saúde passaram por uma transformação disruptiva ao longo dos anos, do papel para computador, web, nuvem, IoT, análise de big data e, finalmente, para blockchain. A segurança e privacidade são grandes preocupações dos sistemas de gerenciamento de dados em saúde baseados em IoT. O requisito de privacidade da identidade de um paciente em um sistema de gerenciamento de dados de saúde é fundamental com o crescente número de fraudes médicas e medicamentos falsos.

Embora os dispositivos IoT permitam o monitoramento contínuo dos dados de saúde, aumentam a complexidade dos pontos de coleta de dados e tornam mais difícil determinar exatamente o que, o porquê e como os dados estão sendo coletados. Isso é especialmente problemático quando se considera o contexto das tecnologias AAL (Active Assisted Living - que são tecnologias de informação e comunicação aplicadas na vida cotidiana, visando apoiar a vida independente e saudável para melhorar a qualidade de vida), por exemplo, os idosos são uma população vulnerável que tradicionalmente não possui conhecimento tecnológico avançado. Fadrique et al (Fadrique et al., 2020) ressaltam que a facilidade no uso dessa tecnologia, a aceitação do usuário e a privacidade de dados devem ser consideradas para fornecer essa solução de forma sustentável.

Para projetar uma rede inteligente de assistência à saúde baseada em 5G, Ahad e colaboradores (Ahad et al., 2020) destacaram os pontos que devem ser considerados para o sucesso, tal como uma comunicação segura e direta deve ser fornecida entre os dispositivos de saúde inteligentes e o centro de banco de dados

em nuvem para autenticidade e integridade dos dados; uma abordagem bem definida deve ser fornecida para avaliação de risco, para detectar ataques futuros e presentes e; uma política de privacidade forte deve ser fornecida para a aprovação e confiança do novo usuário.

Técnicas empregadas para garantia da privacidade em IoT em saúde

O uso efetivo da IoT na saúde leva ao compartilhamento de uma grande quantidade de dados, inclusive dados pessoais, e apesar da facilidade e praticidade das tecnologias da IoT, a privacidade deve ser garantida desde a concepção dos produtos. A incorporação dos princípios da privacidade dos dados no processo de desenvolvimento das tecnologias da IoT é um ponto importante para o avanço desta tecnologia. A seguir, serão descritos o estado da arte das técnicas que estão sendo empregadas atualmente para este fim.

A tecnologia blockchain, nos últimos tempos, tem sido inserida no domínio da saúde para atender à necessidade de um sistema de suporte mais centrado no paciente para os profissionais e para conectar sistemas díspares a fim de melhorar o atendimento ao paciente (Chang e Li, 2019)(Obour Agyekum et al., 2019). Os autores (Radanliev et al., 2020) (Shu et al., 2020) (Jamil et al., 2020) (Rauf et al., 2020) (Taralunga e Florea, 2021) (Ejaz et al., 2021) reforçam o uso da tecnologia blockchain considerando a vantagem de que os pacientes podem transmitir registros pessoais sem o risco de adulteração, pois as regras de bloqueios são imutáveis e rastreáveis. O uso do recurso de rastreabilidade do blockchain garante que os dados usados para desenvolver modelos preditivos sejam precisos, levando a um prognóstico bastante confiável (Segarra et al., 2019).

As técnicas mais aplicadas para abordar as preocupações de privacidade dos dados de saúde do paciente na nuvem são IBE (Identity Based Encryption), ABE (Attribute Based Encryption) e suas variantes (Sajid e Abbas, 2016). Em vez de usar uma metodologia ou solução, como apenas ABE, deve-se concentrar em abordagem multitecnologia, na combinação de várias soluções para alcançar a privacidade refinada, eficiente e soluções escaláveis para manter os dados de cuidados em saúde com segurança no ambiente de nuvem.

Conforme estudos (Ali et al., 2020) (Jeong e Sim, 2021), o blockchain na área de saúde oferece responsabilidade, gerenciamento de identidade e um meio para manter as informações de registro de saúde dos pacientes. Nenhum dos dados reais de monitoramento da saúde dos pacientes são armazenados em blockchain, e os acordos sobre a natureza dos dados que estão sendo compartilhados são mantidos criptografados. Acredita-se que os dados de saúde dos pacientes não estão acessíveis a qualquer pessoa no sistema de monitoramento de saúde, exceto o médico com quem se destina a ser compartilhado. Com a criptografia de ponta

V.11, n.8, 2024. ISSN n° 2359-3652

a ponta, os dados de saúde dos pacientes não podem ser acessados, uma autenticação robusta fornece segurança, privacidade e eficiência (Deng et al., 2017).

Além disso, o uso de blockchain para gerenciamento de consentimento em saúde fornece imutabilidade e descentralização, permitindo maior transparência entre os processos (Velmovitsky et al., 2020) (Giordanengo, 2019) (Griggs et al., 2018) (Kakarlapudi e Mahmoud, 2021).

Estudos relataram o uso de criptografia para garantir a segurança e privacidade dos dados manipulados por dispositivos habilitados para IoT (Ullah et al., 2020) (Segarra et al., 2020) (Angeletti et al., 2018) (Tahir et al., 2018) (Jiang e Shi, 2021) (Kang et al., 2021) (Andreas et al., 2021) (Li et al., 2021) (Pistono et al., 2019) (Jegadeesan et al., 2019), como o trabalho dos autores (Omala et al. 2016) (Omala et al., 2018) que sugerem um esquema de criptografia leve e sem certificado para transferência de dados em redes corporal sem fio (Wireless Body Area Network – WBAN). Quando compararam a solução apresentada com outras sem esquema de certificado, em termos de consumo de energia, observaram que o esquema baseado em elliptic curve cryptosystem (ECC) não é apenas seguro, mas também adequado para recursos de dispositivos restritos, como WBAN. Entretanto, a proposta gera texto cifrado maior do que o esquema proposto por Barbosa e Farshim (BF) e Yin e Liang (YL), que consome menos energia durante Signcrypt.

Hamici (Hamici, 2018) propôs um dispositivo de tele monitoramento biomédico com criptografia genética de alto nível para uso em WBSM/IoT a fim de garantir a privacidade dos dados durante o trânsito na Internet. A criptografia de ácido nucléico é um método emergente e muito promissor na direção da pesquisa de criptografia para a segurança dos dados.

Outro esquema que integra kd-tree com a técnica de criptografia homomórfica para dados armazenados em nuvem foi proposto por Zheng e colaboradores (Zheng et al., 2019). Os autores observaram que o esquema é mais eficiente em termos de consulta k-NN para preservar a privacidade. A segurança do modelo se mostrou satisfatória, eficiente e baixo custo computacional.

Um esquema de autenticação mútua leve é proposto por Jan (Jan et al., 2021) para preservar a privacidade dos dispositivos vestíveis (dispositivos eletrônicos com microcontroladores que são utilizados próximos ou na superfície da pele) e seus dados em um ambiente I-CPS (sistemas ciberfísicos industriais). O esquema é baseado no modelo de interação cliente-servidor que usa criptografia simétrica para estabelecer sessões seguras entre as entidades que se comunicam. Após a autenticação mútua, o risco de privacidade associado aos dados de um paciente é previsto usando um modelo de Markov oculto habilitado para IA.

No estudo de Masud (Masud et al., 2021) são utilizadas várias chaves formadas por meio da função de derivação de chave (KDF) para garantir a criptografia de

ponta a ponta das informações para evitar o uso indevido. Os direitos de acesso aos serviços na nuvem são assegurados com base na identidade e na associação entre as partes interessadas, garantindo assim a privacidade.

Os autores (Krall et al., 2020) apresentam uma abordagem denominada Mosaic Gradient Perturbation (MGP) para preservar a privacidade no âmbito da modelagem preditiva, que atende ao requisito de privacidade diferencial ao mesmo tempo que mitiga o risco de inversão do modelo. O MGP é flexível no ajuste fino das compensações entre o desempenho do modelo e a precisão do ataque, ao mesmo tempo que é altamente escalonável para computação em grande escala.

A privacidade de transmissão das informações pode ser garantida pela implementação do DPWS do padrão WS-Security. Em implementações expostas a segurança pode usar o protocolo HTTPS. Protocolo de autenticação anônima leve foi proposto pelos autores para os requisitos de segurança (Avila et al., 2017).

Para Meena e colaboradores (Meena et al., 2021), os dados relacionados com aplicativos de saúde são principalmente privados e devem estar prontamente disponíveis para os usuários. Aplicar essas duas restrições no ambiente de nuvem é uma tarefa difícil. A computação em névoa é uma arquitetura emergente para fornecer serviços de computação, armazenamento, controle e rede nas proximidades do usuário. Para lidar com dados privados, os elementos de processamento devem ser entidades confiáveis no ambiente em névoa. Para isso, foi proposta uma nova técnica de computação flutuante para aplicativos confiáveis usando computação em névoa, como exposto.

Em outro contexto de aplicação das técnicas de Inteligência Artificial (Car et al., 2019), o estudo de Nadian-Ghomsheh (Nadian-ghomsheh et al., 2021) propõem uma arquitetura IoT holística, hierárquica e com preservação de privacidade para avaliação de reabilitação de mãos com base em técnicas de visão de máquina. O estudo também apresenta novas técnicas de Machine Learning para analisar o progresso dos pacientes durante a fase de reabilitação, e a incorporação de técnicas como Federated Learning, a Privacidade Diferencial e técnicas de compartilhamento de segredos para preservar a privacidade dos proprietários de dados. Combinar os recursos de computação de borda (edge computing), computação de névoa (fog computing), e computação em nuvem (cloud computing) cria um paradigma IoT hierárquico, ou seja, Edge-Fog-Cloud para melhorar o funcionamento da saúde IoT.

Pandemia da COVID-19 e o uso da IoT

Embora as pandemias exijam uma resposta global rápida, Radanliev et al (Radanliev et al., 2020) ponderam que nem todos os países têm a capacidade de

controlar resposta à epidemia de acordo com as políticas de preservação da privacidade. As nações tecnologicamente avançadas têm vantagem neste campo, e poderiam ser mais rápidas em usar esses recursos para fazer impulsionar a governança da saúde digital no mundo. Além de, expandir esses sistemas e ferramentas de dados interoperáveis, fortalecer a governança de dados, bem como criar capacidade para coletar e interpretar dados. Entretanto, poucos estudos abordam sobre a governança digital, com estabelecimentos de políticas, diretrizes e normas dessas tecnologias nas organizações de saúde no contexto público e privado.

Como o cenário da COVID-19 requer soluções particulares para impulsionar o processo de atendimento de emergência e segurança nos dados gerados em todos os ambientes, Verri Lucca e colaboradores (Verri lucca et al., 2020) propuseram uma taxonomia que foi projetada para apoiar o desenvolvimento de mecanismos de privacidade para ambientes de saúde. A principal contribuição da pesquisa consistiu na análise de diferentes parâmetros de privacidade com um aplicativo móvel que considera as diferentes regras propostas na taxonomia.

Na revisão de Asadzadeh e colaboradores (Asadzadeh et al., 2020) mostraram a aplicação das tecnologias da informação e comunicação na pandemia de COVID-19 classificando-a em 4 tópicos (detecção e diagnóstico; abordagem de tratamento; estratégias de proteção e; objetivos do manejo). Destacaram que a IOT foi utilizada, principalmente, para detecção e diagnóstico, bem como nas estratégias de proteção em diferentes locais, como aeroportos, terminais de ônibus e organizações de saúde em cidades inteligentes. E, o uso desses dispositivos para coleta de dados e informações, monitoramento ou rastreamento de pacientes, monitoramento de regiões infectadas e o compartilhamento de informação.

Além disso, Celesti e colaboradores (Celesti et al., 2020) relatam a necessidade do serviço de telessaúde para reduzir a movimentação de pacientes diminuindo, assim, o risco de infecção em uma situação de pandemia. O estudo propõe um serviço de laboratório telemédico, em que exames clínicos são realizados em pacientes diretamente em um hospital por técnicos, e por meio de dispositivos médicos IoT, e os resultados são enviados automaticamente pelo hospital para os médicos de hospitais federados para validação, utilizando a tecnologia blockchain.

Governança Digital e Proteção de Dados Pessoais

Com o avanço da pandemia do Coronavírus, diferentes países introduziram soluções inovadoras para tentar superar o problema, aprimorando as tecnologias digitais de saúde (Unruh et al., 2021). Com isso governança digital e gestão dos dados em saúde entraram em pauta dentro das organizações em todo o mundo. Alami et al., 2017 já haviam destacado que a saúde digital poderia ser “pedra angular” de uma reforma bem-sucedida para melhorar a eficiência e eficácia dos sistemas de saúde em benefício das pessoas. Entretanto, a temática da

governança digital para os dispositivos inteligentes é pouco abordada na literatura a fim de entender como os países e organizações estão tratando. Então, neste estudo, optou-se por refletir sobre as políticas, normas e instrumentos que podem auxiliar a governança dos dispositivos inteligentes no ecossistema digital em saúde.

Diferentes mecanismos vêm sendo aperfeiçoados a fim de garantir que os dados sejam gerenciados corretamente, de acordo com políticas e práticas recomendadas. Desde 2011, no Brasil, o governo vem definindo e publicando instrumentos, que promovam o valor dos dados como ativos estratégicos no processo de transformação digital. Destaca-se a instituição da Política de Governança Digital (Decreto nº 8.638/2016), Política de Dados Abertos (Decreto nº 8.777/2016) e a Estratégia de Saúde Digital para o Brasil (Brasil, 2020).

Diante disso, desenvolver e apoiar iniciativas tecnológicas aplicadas à saúde e aos dispositivos inteligentes, que coletam e armazenam informações de forma automática como IOT, estão na agenda pública para configurar um ecossistema de inovação em saúde, possibilitando o desenho e utilização de soluções que apoiem os profissionais de saúde, gestores e cidadãos (Brasil, 2020).

Um importante desafio para a coleta, organização, gestão, utilização e disponibilização desses dados sobre os indivíduos perpassa por garantir a governança de dados transparentes, devido à sensibilidade dos dados pessoais que precisam ser gerenciados e manipulados de forma segura e responsável

Pesquisadores apontam para a necessidade de redução de situações de conflitos público e privado para uma tutela efetiva à proteção da privacidade no acesso aos dados pessoais (Ventura e Coeli, 2018). Ainda marcam que há a necessidade de ultrapassar as formulações simples de proteção formal dos dados pessoais e procurar alternativas de produção de um bem comum de interesse público na saúde, integrado aos contextos normativos, sociais e políticos nacional e local.

As informações sobre a saúde do indivíduo pertencem a ele e somente podem ser usadas com seu consentimento. Sendo assim, implementar regras fortes e específicas, bem como engajar os atores sobre o tema é uma questão fundamental, uma vez que o uso das tecnologias da IoT envolve a interoperabilidade de dados entre distintos dispositivos.

Nesse contexto, por ser uma preocupação crescente para as nações, diversas regulamentações que visam o fortalecimento das práticas de segurança e privacidade de dados estão sendo aprimoradas. Destacam-se que, os Estados Unidos não possuem uma única lei que governe a privacidade de dados, e sim diversas legislações específicas para diferentes setores ou vigentes em determinado estado. Para os dados de saúde, aplica-se a Health Insurance Portability and Accountability Act (HIPAA), criada em 1996, sendo uma lei

V.11, n.8, 2024. ISSN n° 2359-3652

federal para proteção das informações protegidas de saúde do indivíduo e define regras e limites sobre quem pode acessar as informações (Health Information Privacy, 2022).

Criada no ano de 2000, a Personal Information Protection and Electronic Documents Act (PIPEDA) é uma legislação nacional do Canadá, que tratada das questões mais abrangentes de privacidade e proteção de dados no país (González, 2020). Na Alemanha, em 2017, foi estabelecida a Lei Federal de Proteção de Dados Bundesdatenschutzgesetz (BDSG), que seguem os preceitos da legislação da união europeia.

A General Data Protection Regulation (GDPR), criada em 2018, regulamenta a proteção de dados dos países que pertencem a União Europeia. Refere-se a um projeto de regulação que faz parte de uma série de iniciativas com foco na proteção do usuário, regulamentando o cumprimento de direitos e deveres de pessoas físicas e jurídicas no meio digital (European Commission, 2016).

No que concerne à proteção de dados no Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018 com vigência a partir de 2020, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo (Brasil, 2018). A leia trata sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, abrangendo um composto de operações que podem ocorrer em meios manuais ou digitais. Com isso, o país passou a fazer parte de um grupo de países que contam com uma legislação específica para a proteção de dados dos seus cidadãos (Brasil, 2018).

O impacto maior de uma lei sobre proteção de dados pessoais é o equilíbrio das diferenças de poder sobre o titular dos dados pessoais e aqueles que usam e compartilham as informações pessoais (Ministério Público Federal, 2022), isto é, possibilita que o cidadão tenha controle sobre como suas informações são utilizadas por organizações, empresas e pelo governo (Serpro, 2022).

Cabe ressaltar outro elemento essencial da LGPD, que é o Consentir, ou seja, o consentimento do cidadão é a base para que dados pessoais possam ser tratados. Mas, há algumas exceções a isso. É possível tratar dados sem consentimento se isso for indispensável e estiver especificado na lei (Brasil, 2018) (Serpro, 2022).

Dados pessoais sensíveis podem estar sendo coletados por dispositivos IoT, e o armazenamento e processamento de tais dados devem ser realizados segundo as regras impostas pela LGPD, pois se enquadram no escopo da lei. No desenvolvimento de IoT em conformidade com a lei, é possível citar vazamentos de dados, dificuldade de obter consentimento do usuário, uso de dados para fins diferentes daqueles para os quais foram inicialmente coletados e o esforço para a anonimização de dados como desafios do tratamento de dados (Vojkovi? et al., 2020).

Portanto, a governança digital e a proteção de dados pessoais devem ser o carro chefe das organizações públicas e privadas no Brasil, no sentido de impulsionar o avanço da normatização, avaliação e consolidação de um ecossistema de inovação digital para o sistema de saúde.

CONCLUSÃO

Neste trabalho foi possível observar que a Internet das Coisas possibilita maior integração entre os diferentes pontos de atenção da rede de saúde, possibilitando que a atenção primária à saúde se torne mais acessível e os cuidados de saúde secundários e terciários mais proativos, contínuos e coordenados.

No entanto, a IoT possui requisitos específicos no que tange aos aspectos de privacidade, tendo em vista que possui um ambiente heterogêneo com um número maior de dispositivos ativos e conectados à internet, que podem ser afetados por falhas de segurança. A combinação de informações e acessos registrados nos dispositivos inteligentes pode colocar à privacidade em risco nos casos de exposição de dados indevidamente. Por esses motivos, os principais desafios atuais são a segurança e proteção na coleta e compartilhamento de dados pessoais de saúde, bem como a governança desse ecossistema.

Constatou-se que há pouca produção científica que aborda a governança digital dos dispositivos habilitados para IOT dentro do ecossistema digital de saúde, necessitando ser aprofundada como forma de estabelecer diretrizes, normas e práticas que possibilitem o uso e os avanços dessa tecnologia no apoio à saúde.

A revisão demonstrou que é imprescindível conciliar os avanços dos novos paradigmas apresentados pela IoT com o grande volume de dados em saúde gerados pelos dispositivos inteligentes. Os dispositivos são vistos como novas portas de entrada para os sistemas, em que se faz necessária a garantia da privacidade dos dados em saúde, objetivando a preservação das informações pessoais e privadas dos usuários. Contudo, a temática privacidade de dados de saúde ainda apresenta uma lacuna no sentido de entender como os desenvolvedores e autoridades de saúde estão trabalhando conjuntamente a legislação para garantir o sigilo da coleta, tratamento e compartilhamento dos dados pessoais. Estabelecer comunicação com os usuários desses dispositivos é importante para garantir uma estrutura política de IoT, legítima e eficaz, possibilitando que os usuários tenham papel proativo no controle dos dados pessoais e serviços de IoT.

O tema também desencadeia a discussão da necessidade do uso de dados pessoais da saúde para construção de parâmetros utilizados na definição de políticas públicas para atendimento do interesse coletivo, ou seja, o uso de forma a garantir a satisfação de necessidades coletivas. Ainda, o tema traz a necessidade de entender na literatura a associação da privacidade e segurança

V.11, n.8, 2024. ISSN n° 2359-3652

dos dados, arquitetura, tecnologia e métodos utilizados para garantir a díade. Trabalho futuro está em processo de elaboração pelos autores deste artigo para complementação da temática abordando os aspectos relativos à segurança de dados.

Esta revisão possui limitações que devem ser destacadas, como a busca somente na base de dados PubMed que pode não ter abarcado pesquisas relevantes por estarem em bases de dados que não foram utilizadas. Além disso, não é possível abordar todos os métodos aplicados para privacidade desses tipos de dispositivos.

Espera-se, assim, que as contribuições presentes neste artigo possam orientar diretrizes e regulamentações aplicáveis à proteção da privacidade dos dados em saúde produzidos pelos dispositivos inteligentes da IoT, para serem adotadas na complexa tarefa da assistência à saúde, bem como na promoção de um instrumento de acesso à informação para aplicação no setor saúde e apoio em epidemias.

Referências

AHAD, A.; TAHIR, M.; AMAN SHEIKH, M.; AHMED, K. I.; MUGHEES, A.; MUGHEES, A. Technologies Trend towards 5G Network for Smart Health-Care Using IoT: A Review. **Sensors (Basel, Switzerland)**, v. 20, n. 14, jul. 2020.

ALAMI, H.; GAGNON, M.-P.; FORTIN, J.-P. Digital health and the challenge of health systems transformation. **mHealth**, v. 3, p. 31–31, 2017.

ALI, M. S.; VECCHIO, M.; PUTRA, G. D.; KANHERE, S.S.; ANTONELLI, F. A Decentralized Peer-to-Peer Remote Health Monitoring System. **Sensors (Basel, Switzerland)**, v. 20, n. 6, mar. 2020.

ANDREAS, A.; MAVROMOUSTAKIS, C. X.; MASTORAKIS, G.; DO, D.; BATALLA, J. M.; PALLIS, E.; MARKAKIS, E. K. Towards an optimized security approach to IoT devices with confidential healthcare data exchange. **Multimedia tools and applications**, p. 1–15, mar. 2021.

ANGELETTI, F.; CHATZIGIANNAKIS, I.; VITALETTI, A. Towards an architecture to guarantee both data privacy and utility in the first phases of digital clinical trials. **Sensors (Switzerland)**, v. 18, n. 12, 2018.

ASADZADEH, A.; PAKKHOO, S.; SAEIDABAD, M. M.; KHEZRI, H.; FERDOUSI, R. Information technology in emergency management of COVID-19 outbreak. **Informatics in Medicine Unlocked**, v. 21, p. 100475, 2020.

AVILA, K.; FERDOUSI, R.; JABBA, D.; JIMENO, M. Applications based on service-oriented architecture (SOA) in the field of home healthcare. **Sensors (Switzerland)**, v. 17, n. 8, 2017.

BRASIL. Lei 13.709 de 14 de agosto de 2018. . 2018.

BRASIL. **Estratégia de Saúde Digital para o Brasil 2020-2028**. [s.l: s.n.].

CAR, J.; SHEIKH, A.; WICKS, P.; WILLIAMS, M. S. **Beyond the hype of big data and artificial intelligence: building foundations for knowledge and wisdom.BMC medicine**, jul. 2019.

CELESTI, A.; RUGGERI, A.; FAZIO, M.; GALLETTA, A.; VILLARI, M.; ROMANO, A. Blockchain-Based Healthcare Workflow for Tele-Medical Laboratory in Federated Hospital IoT Clouds. **Sensors (Basel, Switzerland)**, v. 20, n. 9, maio 2020.

CHANG, C.-C.; LI, C.-T. Algebraic secret sharing using privacy homomorphisms for IoT-based healthcare systems. **Mathematical biosciences and engineering : MBE**, v. 16, n. 5, p. 3367–3381, abr. 2019.

DASH, S. P. The Impact of IoT in Healthcare: Global Technological Change & The Roadmap to a Networked Architecture in India. **Journal of the Indian Institute of Science**, v. 100, n. 4, p. 773–785, 2020.

DENG, Y. Y.; CHEN, C. L.; TSAUR, W. J.; TANG, Y. W.; CHEN, J. H. Internet of things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system. **Sensors (Switzerland)**, v. 17, n. 12, 2017.

DEY, N.; ASHOUR, A. S.; SHI, F.; FONG, S. J.; TAVARES, J. M. R. S. Medical cyber-physical systems: A survey. **Journal of medical systems**, v. 42, n. 4, p. 74, mar. 2018.

DHINGRA, D.; DABAS, A. Global Strategy on Digital Health. **Indian Pediatrics**, v. 57, n. 4, p. 356–358, 2020.

EJAZ, M.; KUMAR, T.; KOVACEVIC, I.; YLIANTTILA, M.; HARJULA, E. Health-BlockEdge: Blockchain-Edge Framework for Reliable Low-Latency Digital Healthcare Applications. **Sensors (Basel, Switzerland)**, v. 21, n. 7, abr. 2021.

EL-HAJJ, M.; FADLALLAH, A.; CHAMOUN, M.; SERHROUCHNI, A. A Survey of Internet of Things (IoT) Authentication Schemes. **Sensors (Basel, Switzerland)**, v. 19, n. 5, mar. 2019.

EUROPEAN COMMISSION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. . 2016.

FADRIQUE, L. X.; RAHMAN, D.; VAILLANCOURT, H.; BOISSONNEAULT, P.; DONOVSKA, T.; MORITA, P. P. Overview of Policies, Guidelines, and Standards for Active Assisted Living Data Exchange: Thematic Analysis. **JMIR mHealth and uHealth**, v. 8, n. 6, p. e15923, jun. 2020.

GIORDANENGO, A. Possible Usages of Smart Contracts (Blockchain) in Healthcare and Why No One Is Using Them. **Studies in health technology and informatics**, v. 264, p. 596–600, ago. 2019.

GONZÁLEZ, M. **Conheça o cenário das leis de proteção de dados ao redor do mundo**. Disponível em: <https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/>.

GOPE, P.; GHERAIBIA, Y.; KABIR, S.; SIKDAR, B. A Secure IoT-Based Modern Healthcare System With Fault-Tolerant Decision Making Process. **IEEE journal of biomedical and health informatics**, v. 25, n. 3, p. 862–873, mar. 2021.

GRIGGS, K. N.; OSSIPOVA, O.; KOHLIOS, C. P.; BACCARINI, A. N.; HOWSON, E. A.; HAYAJNEH, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. **Journal of Medical Systems**, v. 42, n. 7, p. 1–7, 2018.

HAMICI, Z. Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways. **IEEE journal of biomedical and health informatics**, v. 22, n. 6, p. 1814–1823, nov. 2018.

HARRIS, P. A.; TAYLOR, R.; THIELKE, R.; JONATHON, P.; GONZALEZ, N.; G, C. J. Research electronic data capture (REDCap)—A metadata-driven methodology and workflow process for providing translational research informatics support. **Journal of Biomedical Informatics**, v. 42, n. 2, p. 377–381, 2009.

HARRIS, P. A.; TAYLOR, R; MINOr, B. L.; ELLIOTT, V.; FERNANDEZ, M.; O'NEAL, L.; MCLEOD, L.; DELACQUA, G.; DELACQUA, F.; KIRBY, J.; DUDA, S. N. The REDCap consortium: Building an international community of software platform partners. **Journal of Biomedical Informatics**, v. 95, p. 103208, 2019.

HEALTH INFORMATION PRIVACY. **What does the HIPAA Privacy Rule do?** Disponível em: <https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html>.

HENRIQUES, D.; PEREIRA, R. F.; ALMEIDA, R.; MIRA DA SILVA, M. IT governance enablers in relation to IoT implementation: a systematic literature review. **Digital Policy, Regulation and Governance**, v. 22, n. 1, p. 32–49, 2020.

HUSSAIN, F.; ABBAS, S. G.; SHAH, G. A.; PIRES, I. M.; FAYYAZ, U. U.; SHAHZAD, F.; GARCIA, N. M.; ZDRAVEVSKI, E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. **Sensors (Basel, Switzerland)**, v. 21, n. 9, abr. 2021.

ISMAIL, L.; MATERWALA, H.; K., ACHIM P.; ADEM, A. Requirements of Health Data

Management Systems for Biomedical Care and Research: Scoping Review. **Journal of medical Internet research**, v. 22, n. 7, p. e17508, jul. 2020.

JAMIL, F.; ADEM, A.; IQBAL, N.; KIM, D. H. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. **Sensors (Basel, Switzerland)**, v. 20, n. 8, abr. 2020.

JAN, M. A.; KHAN, F.; KHAN, R.; MASTORAKIS, S.; MENON, V. G.; ALAZAB, M.; WATTERS, P. A Lightweight Mutual Authentication and Privacy-preservation Scheme for Intelligent Wearable Devices in Industrial-CPS. **IEEE transactions on industrial informatics**, v. 17, n. 8, p. 5829–5839, ago. 2021.

JEGADEESAN, S.; DHAMODARAN, M.; AZEES, M.; SHANMUGAPRIYA, S. S. Computationally efficient mutual authentication protocol for remote infant incubator monitoring system. **Healthcare technology letters**, v. 6, n. 4, p. 92–97, ago. 2019.

JEONG, Y.-S.; SIM, S.-H. Hierarchical Multipath Blockchain Based IoT Information Management Techniques for Efficient Distributed Processing of Intelligent IoT Information. **Sensors (Basel, Switzerland)**, v. 21, n. 6, mar. 2021.

JIANG, D.; SHI, G. Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. **Journal of healthcare engineering**, v. 2021, p. 6656204, 2021.

JOHN, J.; VARKEY, M. S.; SELVI, M. Security attacks in s-wbans on iot based healthcare applications. **Int. J. Innovative Technol. Explor. Eng**, v. 9, n. 1, p. 2088–2097, 2019.

KAKARLAPUDI, P. V.; MAHMOUD, Q. H. A Systematic Review of Blockchain for Consent Management. **Healthcare (Basel, Switzerland)**, v. 9, n. 2, fev. 2021.

KANG, J. J.; DIBAEI, M.; LUO, G.; YANG, W.; HASKELL-DOWLAND, P.; ZHENG, X. An Energy-Efficient and Secure Data Inference Framework for Internet of Health Things: A Pilot Study. **Sensors (Basel, Switzerland)**, v. 21, n. 1, jan. 2021.

KELLY, J. T.; CAMPBELL, K. L.; GONG, E.; SCUFFHAM, P. The Internet of Things: Impact and Implications for Health Care Delivery. **Journal of medical Internet research**, v. 22, n. 11, p. e20135, nov. 2020.

KRALL, A.; FINKE, D.; YANG, H. Mosaic Privacy-preserving Mechanisms for Healthcare Analytics. **IEEE journal of biomedical and health informatics**, v. PP, nov. 2020.

LAPLANTE, P. A.; KASSAB, M.; LAPLANTE, N. L.; VOAS, J. M. Building Caring Healthcare Systems in the Internet of Things. **IEEE systems journal**, v. 12, n. 3, 2018.

LI, H.; YU, K.; LIU, B.; FENG, C.; QIN, Z.; SRIVASTAVA, G. An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things. **IEEE journal of biomedical and health informatics**, v. PP, abr. 2021.

MARTÍN-RUÍZ, M. L.; FERNÁNDEZ-ALLER, C.; PORTILLO, E.; MALAGÓN, J.; DEL BARRIO, C. Developing a System for Processing Health Data of Children Using Digitalized Toys: Ethical and Privacy Concerns for the Internet of Things Paradigm. **Science and engineering ethics**, v. 24, n. 4, p. 1057–1076, ago. 2018.

MASUD, M.; GABA, G. S.; CHOUDHARY, K.; ALROOBAEA, R.; HOSSAIN, M. S. A robust and lightweight secure access scheme for cloud based E-healthcare services. **Peer-to-peer networking and applications**, p. 1–15, maio 2021.

MEENA, V.; GORRIPATTI, M.; SURIYA PRABA, T. Trust Enforced Computational Offloading for Health Care Applications in Fog Computing. **Wireless personal communications**, p.

1–18, abr. 2021.

MINISTÉRIO PÚBLICO FEDERAL. **Lei Geral de Proteção de Dados**. Disponível em: <http://www.mpf.mp.br/servicos/lgpd>.

MONTEITH, S.; GLENN, T.; GEDDES, J.; SEVERUS, E.; WHYBROW, P. C.; BAUER, M. Internet of things issues related to psychiatry. **International Journal of Bipolar Disorders**, v. 9, n. 1, 2021.

MRABET, H.; BELGUITH, S.; ALHOMOUD, A.; JEMAI, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. **Sensors (Basel, Switzerland)**, v. 20, n. 13, jun. 2020.

NADIAN-GHOMSHEH, A.; FARAHANI, B.; KAVIAN, M. A hierarchical privacy-preserving IoT architecture for vision-based hand rehabilitation assessment. **Multimedia tools and applications**, p. 1–24, fev. 2021.

NIŽETIĆ, S.; ŠOLIĆ, P.; LÓPEZ-DE-IPIÑA GONZÁLEZ-DE-ARTAZA, D.; PATRONO, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. **Journal of cleaner production**, v. 274, p. 122877, nov. 2020.

OBOUR AGYEKUM, K. O.-B.; XIA, Q.; SIFAH, E. B.; GAO, Jianbin.; XIA, H.; DU, X.; GUIZANI, M. A Secured Proxy-Based Data Sharing Module in IoT Environments Using Blockchain. **Sensors (Basel, Switzerland)**, v. 19, n. 5, mar. 2019.

OMALA, A. A.; MBANDU, A. S.; MUTIRIA, K. D.; JIN, C.; LI, F. Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. **Journal of medical systems**, v. 42, n. 6, p. 108, abr. 2018.

OMALA, A. A.; ROBERT, N.; LI, F. A Provably-Secure Transmission Scheme for Wireless Body Area Networks. **Journal of Medical Systems**, v. 40, n. 11, 2016.

PISTONO, M.; BELLAFQIRA, R.; COATRIEUX, G. Secure Processing of Stream Cipher Encrypted Data Issued from IOT: Application to a Connected Knee Prosthesis. **Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference**, v. 2019, p. 6494–6497, jul. 2019.

RADANLIEV, P.; DE ROURE, D.; WALTON, R.; VAN KLEEK, M.; MONTALVO, R. M.; SANTOS, O.; MADDOX, L. T.; CANNADY, S. COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. **The EPMA journal**, v. 11, n. 3, p. 311–332, set. 2020.

RAUF, A.; WANG, Z.; SAJID, H.; ALI TAHIR, M. Secure Route-Obfuscation Mechanism with Information-Theoretic Security for Internet of Things. **Sensors (Basel, Switzerland)**, v. 20, n. 15, jul. 2020.

RYU, J.; KANG, D.; LEE, H.; KIM, H.; WON, D. A Secure and Lightweight Three-Factor-Based Authentication Scheme for Smart Healthcare Systems. **Sensors (Basel, Switzerland)**, v. 20, n. 24, dez. 2020.

SAJID, A.; ABBAS, H. Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges. **Journal of medical systems**, v. 40, n. 6, p. 155, jun. 2016.

SCHUKAT, M.; MCCALDIN, D.; WANG, K.; SCHREIER, G.; LOVELL, N. H.; MARSCHOLLEK, M.; REDMOND, S. J. Unintended Consequences of Wearable Sensor Use in Healthcare. Contribution of the IMIA Wearable Sensors in Healthcare WG. **Yearbook of medical informatics**, n. 1, p. 73–86, nov. 2016.

SEGARRA, C.; MUNTANE, E.; LEMAY, M.; SCHIAVONI, V.; DELGADO-GONZALO, R. Secure Stream Processing for Medical Data. **Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference**, v. 2019, p. 3450–3453, jul. 2019.

SEGARRA, C.; DELGADO-GONZALO, R.; SCHIAVONI, V. MQT-TZ: Secure MQTT Broker for Biomedical Signal Processing on the Edge. **Studies in health technology and informatics**, v. 270, p. 332–336, jun. 2020.

SERPRO. **Serpro e LGPD: segurança e inovação**. Disponível em: <https://www.serpro.gov.br/lgpd/>.

SHU, H.; QI, P.; HUANG, Y.; CHEN, F.; XIE, D.; SUN, L. An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based Medical Cyber Physical Systems. **Sensors (Basel, Switzerland)**, v. 20, n. 5, mar. 2020.

TAHIR, H.; TAHIR, R.; MCDONALD-MAIER, K. On the security of consumer wearable devices in the Internet of Things. **PloS one**, v. 13, n. 4, p. e0195487, 2018.

TARALUNGA, D. D.; FLOREA, B. C. A Blockchain-Enabled Framework for mHealth Systems. **Sensors (Basel, Switzerland)**, v. 21, n. 8, abr. 2021.

ULLAH, I.; AMIN, N. U.; KHAN, M. A.; KHATTAK, H.; KUMARI, S. An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. **Journal of medical systems**, v. 45, n. 1, p. 4, nov. 2020.

UNRUH, L.; ALLIN, S.; MARCHILDON, G.; BURKE, S.; BARRY, S.; SIERSBAEK, R.; THOMAS, S.; RAJAN, S.; KOVAL, A.; ALEXANDER, M.; MERKUR, S.; WEBB, E.; WILLIAMS, G. A. A comparison of 2020 health policy responses to the COVID-19 pandemic in Canada, Ireland, the United Kingdom and the United States of America. **Health Policy**, v. 126, p. 427–437, 2021.

VELMOVITSKY, P. E.; MIRANDA, P. A. S. S.; VAILLANCOURT, H.; DONOVSKA, T.; TEAGUE, J.; MORITA, P. P. A Blockchain-Based Consent Platform for Active Assisted Living: Modeling Study and Conceptual Framework. **Journal of medical Internet research**, v. 22, n. 12, p. e20832, dez. 2020.

VENTURA, M.; COELI, C. M. Beyond privacy: The right to health information, personal data protection, and governance. **Cadernos de Saude Publica**, v. 34, n. 7, p. 7–10, 2018.

VERDEJO ESPINOSA, Á.; LOPEZ RUIZ, J.; MATA MATA, F.; ESTEVEZ, M. E. Application of IoT in Healthcare: Keys to Implementation of the Sustainable Development Goals. **Sensors (Basel, Switzerland)**, v. 21, n. 7, p. 2330, 26 mar. 2021.

VERRI LUCCA, A.; AUGUSTO SILVA, L.; LUCHTENBERG, R.; GARCEZ, L.; MAO, X.; GARCÍA OVEJERO, R.; MIGUEL PIRES, I.; LUIS VICTÓRIA BARBOSA, J.; REIS QUIETINHO LEITHARDT, V. A Case Study on the Development of a Data Privacy Management Solution Based on Patient Information. **Sensors (Basel, Switzerland)**, v. 20, n. 21, out. 2020.

VOJKOVI?, G.; MILENKOVI?, M.; KATULI?, T. IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. **Business Systems Research Journal**, v. 11, n. 3, p. 167–185, 2020.

YIN, X. C.; LIU, Z. G.; NDIBANJE, B.; NKENYEREYE, L.; RIAZUL ISLAM, S. M. An iot-based anonymous function for security and privacy in healthcare sensor networks. **Sensors (Switzerland)**, v. 19, n. 14, p. 1–14, 2019.

ZHENG, Y.; LU, R.; SHAO, J. Achieving Efficient and Privacy-Preserving k-NN Query for Outsourced eHealthcare Data. **Journal of medical systems**, v. 43, n. 5, p. 123, mar. 2019.