Processando o Saber
eISSN 2179-5150
FATEC Praia Grande · fatecpg.edu.br/revista
submetido: Jan/2024 · **aceito**: Mar/2024 · **publicado**: Jun/2024

Proteção da privacidade em dispositivos IOT de acordo com a LGPD: Um estudo abrangente

Privacy protection in IOT devices according to LGPD: A comprehensive study

Brian Melinski Bianchini
Fatec Praia Grande
brianmb18@gmail.com

Erik Faria Silva
Fatec Praia Grande
erik.faria.da.silva13@gmail.com

Jônatas Cerqueira Dias
Fatec Praia Grande
jonatas.dias2@fatec.sp.gov.br

RESUMO

A Internet das Coisas (IoT) transformou profundamente a interação humana com o ambiente, conectando dispositivos físicos e automatizando tarefas anteriormente complexas. No entanto, essa revolução tecnológica também levanta preocupações sobre segurança e privacidade, especialmente no tratamento de dados pessoais e sensíveis. O constante crescimento da adoção de dispositivos e sistemas IoT destaca a necessidade de conciliar essa tecnologia com regulamentações específicas, como a Lei Geral de Proteção de Dados (LGPD). O desafio reside na ausência de diretrizes explícitas sobre a manipulação de dados em sistemas IoT nas legislações existentes. Este estudo busca compreender a coexistência da IoT com LGPD, explorando soluções para garantir a segurança e privacidade dos dados em um cenário de rápida evolução tecnológica. A eficácia de *checklists* na verificação de conformidade, a proposta do *Personal Data Storage* (PDS) em conjunto com a IoT, e a aplicação de técnicas de Engenharia de Requisitos Baseada em Objetivos foram abordadas. Além disso, a implementação prática do PDS no contexto do Sistema Único de Saúde (SUS) e a identificação de requisitos funcionais e não funcionais para adequação à LGPD em sistemas IoT na saúde foram discutidas. O estudo destaca a importância de implementar os princípios da LGPD na IoT, preenchendo lacunas regulatórias e promovendo a segurança e privacidade dos dados. A coexistência eficiente desses elementos não apenas atende a requisitos legais, mas também constrói confiança, capacitando os usuários com maior controle sobre seus dados. Inovações contínuas e pesquisas práticas são essenciais para orientar organizações, pesquisadores e legisladores na busca por soluções que preservem a integridade dos dados em um ambiente conectado.

PALAVRAS-CHAVE: Internet das Coisas; Lei Geral de Proteção de Dados Pessoais; Privacidade de Dados; Proteção de Dados.

ABSTRACT

"The Internet of Things (IoT) has profoundly transformed human interaction with the environment by connecting physical devices and automating tasks that were once complex. However, this technological revolution also raises concerns about security and privacy, particularly in the handling of personal and sensitive data. The continuous growth in the adoption of IoT devices and systems underscores the need to reconcile this technology with specific regulations, such as the General Data Protection Law (LGPD). The challenge lies in the absence of explicit guidelines regarding the handling of data in IoT systems within existing legislations. This study aims to comprehend the coexistence of IoT with the LGPD, exploring solutions to ensure the security and privacy of data in a rapidly evolving technological landscape. The effectiveness of checklists in compliance verification, the proposal of the Personal Data Storage (PDS) in conjunction with IoT, and the application of Goal-Oriented Requirements Engineering techniques have been addressed. Furthermore, the practical implementation of PDS in the context of the Unified Health System (SUS) and the identification of functional and non-functional requirements for LGPD compliance in health IoT systems were discussed. The study highlights the importance of implementing LGPD principles in IoT, filling regulatory gaps, and promoting the security and privacy of data. The efficient coexistence of these elements not only meets legal requirements but also builds trust, empowering users with greater control over their data. Continuous innovations and practical research are essential to guide organizations, researchers, and policymakers in the pursuit of solutions that preserve data integrity in a connected environment.".

KEY-WORDS*: Internet of Things; General Data Protection Law; Data Privacy; Data Protection.*

INTRODUÇÃO

A Internet das Coisas (IoT) é uma tecnologia que mudou e continua a transformar a forma como interagimos com o mundo ao nosso redor. Ela ocorre por meio da conexão de dispositivos físicos à internet, permitindo a comunicação entre eles e dando-lhes a capacidade de realizar tarefas que antes exigiam diversos dispositivos independentes, assim como sua automação. De acordo com a perspectiva de Albertin e Albertin (2017), a IoT se baseia na captação, processamento e análise de informações originadas por sensores presentes em diversos objetos, os quais se conectam através da infraestrutura de comunicação pública.

No entanto, devido ao constante crescimento da utilização de dispositivos e sistemas IoT, nasce a preocupação com segurança e privacidade dos dados que são consumidos e utilizados por ela, por envolver uma quantidade massiva de dados pessoais e sensíveis. Como (CHEN et al., 2014) aponta, as redes IoT apresentam desafios de segurança e privacidade mais significativos do que as redes tradicionais. Isso ocorre porque a IoT coleta e processa grandes quantidades de dados pessoais, que podem ser usadas para fins maliciosos. A falta de segurança adequada pode resultar em quebra de privacidade, roubo de identidade etc.

Por isso, é importante que nos preocupemos com a segurança dos dados na IoT. Tais dispositivos devem possuir um alto nível de segurança e estar de acordo com leis, como a Lei Geral de Proteção de Dados (LGPD), e políticas que visam aprimorar a segurança e privacidade dos dados de seus usuários. Além disso, outro fator a ser considerado é a conscientização dos usuários sobre os riscos associados à IoT e o ato de instruí-los sobre as práticas recomendadas para garantir a proteção de seus dados.

A LGPD e a segurança na rede são temas de extrema relevância no contexto atual, em que a digitalização e a coleta de dados pessoais se tornaram parte integrante das atividades cotidianas (CAMARGO PINHO DE ALENCAR, 2023).

A LGPD é um importante marco legislativo que altera consideravelmente o atual modelo de coleta e tratamento indiscriminado de dados pessoais para um modelo em que se realizará a coleta e tratamento somente do necessário (WACHOWICZ, 2020; KOHLS; DUTRA; WELTER, 2021). A LGPD traz consigo os fundamentos que frisam a proteção de direitos e garantias da pessoa natural, como o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, à inviolabilidade da intimidade, ao desenvolvimento econômico e tecnológico, além da livre iniciativa e respeitos aos direitos humanos.

Embora a LGPD não aborde especificamente a manipulação de dados em sistemas de IoT, a implementação de seus princípios e diretrizes pode preencher a lacuna de regularização existente com esta tecnologia (ZEADALLY; BADRA, 2015). Inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE), visa o tratamento de dados. A UE é uma das maiores geradoras de dados do mundo e, por isso, a elaboração de uma legislação para o tratamento desses dados era imprescindível. A LGPD representa uma boa regularização dos termos de dados, embora, tanto a RGPD, quanto a LGPD não abordem especificamente a manipulação de dados em sistemas de IoT[1] (ZEADALLY; BADRA, 2015). Porém, a implementação analógica da lei é viável para evitar a violação de diretrizes de dados pessoais e sensíveis. É necessário utilizar os artigos da LGPD para implementar no âmbito do ecossistema de tratamento automatizado em sistemas de IoT, preenchendo a lacuna de regularização existente.

[1] A LGPD brasileira, em vigor a partir de 18 de setembro de 2020, tem como objetivo principal regulamentar o tratamento de dados pessoais por parte de entidades públicas e privadas. Ela estabelece princípios e diretrizes específicas para garantir a proteção dos direitos e liberdades fundamentais dos titulares de dados. No entanto, ao contrário de seu foco explícito em dados pessoais, a lei não aborda especificamente os desafios e considerações específicas relacionadas à manipulação de dados em sistemas de IoT (ZEADALLY; BADRA, 2015; KOHLS; DUTRA; WELTER, 2021). O RGPD da União Europeia, em vigor a partir de 25 de maio de 2018, tem uma abordagem semelhante à LGPD e foca na proteção dos direitos dos cidadãos em relação ao tratamento de dados pessoais. Embora ambos os regulamentos forneçam orientações valiosas sobre como lidar com dados pessoais, não há disposições detalhadas que se concentrem diretamente nas peculiaridades da manipulação de dados em sistemas de IoT (ZEADALLY; BADRA, 2015; KOHLS; DUTRA; WELTER, 2021)

Nesse contexto este estudo propõe a seguinte questão de pesquisa: “De que forma as restrições da LGPD e preocupações de segurança dos dados relacionadas ao uso da tecnologia IoT podem limitar a capacidade das empresas em transformar os benefícios desta tecnologia em resultados organizacionais efetivos?”

Desta forma, a questão de pesquisa orienta o seguinte objetivo: “Compreender a tecnologia IoT com base nas limitações impostas pela LGPD e buscar na literatura atual soluções que permitam a sociedade se beneficiarem do uso de dados de usuários pelas organizações, ao mesmo tempo que esta proporciona valor de informação a estes mesmos usuários, enquanto as organizações usufruem dos ganhos proporcionados por esta tecnologia.”

Esta pesquisa se justifica diante do crescimento exponencial do uso de dispositivos IoT e das crescentes preocupações relacionadas à segurança e privacidade dos dados. A IoT, embora promissora para transformar nosso modo de vida e trabalho, também apresenta desafios significativos. Nesse cenário, a pesquisa alinha-se às preocupações éticas e legais emergentes relacionadas à utilização da IoT, buscando proporcionar contribuições substanciais tanto para a sociedade quanto para as organizações envolvidas nesse contexto.

A LGPD surge como um marco legislativo importante para salvaguardar os direitos e garantias da pessoa natural no contexto da coleta, uso e tratamento de dados pessoais. No entanto, é importante reconhecer que a LGPD não aborda diretamente os desafios específicos de segurança e privacidade associados à IoT. Alinhando-se ao problema de pesquisa e aos objetivos propostos, este estudo visa explorar possibilidades para mitigar os riscos de quebra de privacidade e vazamento de dados em sistemas de IoT. Mais importante ainda, busca destacar as melhorias na segurança dos dados resultantes da conformidade com as diretrizes da LGPD.

2 FUNDAMENTAÇÃO TEÓRICA

O presente artigo expõe a preocupação relacionada aos riscos da privacidade dos usuários que utilizam dispositivos de IoT. Embora atualmente a segurança da informação (SI), esteja avançada e represente segurança razoável aos dados e privacidade de seus usuários, não é o único fator a ser considerado, também há a necessidade de saber como estes dados estão sendo tratados por aqueles que os coletam, algo que é difícil de saber quando falamos sobre dispositivos e sistemas IoT devido a quantidade massiva de dados coletados por eles, que nem

sempre o usuário tem controle (DE LIMA; DE ALMEIDA; MAROSO, 2020; KOHLS; DUTRA; WELTER, 2021).

Tendo em vistas tais pontos e que com a chegada da LGPD os sistemas e dispositivos não só devem fornecer um maior controle dos dados aos usuários, como aumentar a proteção de sua privacidade por meio das regras e diretrizes estabelecidas pela mesma, será abordado se é como os dados pessoais estão tendo sua privacidade preservada em dispositivos IoT que se encontram em conformidade com a LGPD (ZEADALLY; BADRA, 2015).

2.1 INTERNET DAS COISAS – INTERNET OF THINGS (IOT)

A Internet das Coisas (IoT) representa uma transformação significativa em nossa interação com o ambiente circundante. Essa tecnologia viabiliza a conexão de dispositivos físicos à internet, capacitando a comunicação entre eles e conferindo a habilidade de executar tarefas que, anteriormente, demandariam vários dispositivos independentes, inclusive sua automação. Seguindo a perspectiva de Albertin e Albertin (2017), a IoT fundamenta-se na captação, processamento e análise de informações provenientes de sensores presentes em diversos objetos, conectando-se por meio da infraestrutura de comunicação pública.

A abrangência da IoT exige consideração de duas dimensões essenciais. A dimensão vertical incorpora setores e iniciativas que podem se beneficiar da IoT, enquanto a dimensão horizontal envolve aspectos transversais a todas as utilizações dessa tecnologia (ALBERTIN; ALBERTIN, 2017). As dimensões verticais podem ser agrupadas de maneira geral ou específica, exemplificado pelas cidades inteligentes, que podem ser subdivididas em mobilidade urbana e segurança, entre outras categorias. Além disso, as dimensões horizontais, como segurança, privacidade e infraestrutura, são interligadas a mais de uma vertical, refletindo uma visão abrangente da IoT.

Essa perspectiva da IoT contribui para compreender a interconexão crescente de dispositivos em nosso cotidiano. Ao considerar o papel da IoT na relação com a LGPD, destacamos como a privacidade e a segurança dos dados são fatores cruciais neste ecossistema tecnológico em constante expansão.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD representa um marco legislativo essencial que redefine significativamente o modelo vigente de coleta e tratamento indiscriminado de dados pessoais. Essa legislação reforça os princípios fundamentais que asseguram os direitos e garantias da pessoa natural, destacando aspectos como respeito à privacidade, autodeterminação informativa, liberdade de expressão, inviolabilidade da intimidade, desenvolvimento econômico e tecnológico, além do respeito aos direitos humanos.

Conforme estabelecido pela legislação (BRASIL, 2019), a LGPD concentra-se no tratamento de dados pessoais, abrangendo meios digitais e sendo aplicável a indivíduos, organizações de direito público e privado. É crucial observar que a LGPD não trata de dados relacionados a pessoas jurídicas, informações sigilosas, patentes ou software. Esses temas já encontram regulamentação em diplomas legais específicos, como a Lei de Propriedade Industrial (Lei 9.279/1996), a Lei de *Software* (Lei 9.609/1998) e a Lei dos Direitos Autorais (Lei 9.610/1998).

O alcance da LGPD, conforme descrito no art. 3º, é amplo, aplicando-se a todas as formas de tratamento de dados pessoais, independentemente do meio, da sede da entidade, ou da localização dos dados. A legislação abrange situações em que o tratamento ocorre em território nacional, visando à oferta ou fornecimento de bens ou serviços, ou ao tratamento de dados de indivíduos em território nacional, mesmo que os dados tenham sido coletados em território nacional. Essa abrangência destaca a importância de sua aplicação em um cenário globalizado e digital.

3 MATERIAIS E MÉTODOS

A pesquisa em questão, conforme sua natureza, pode ser classificada como uma pesquisa aplicada de caráter exploratório, pois tem-se como objetivo encontrar uma solução para um problema real existente (GIL, 2002). Uma estratégia com duas abordagens foi adotada: a primeira envolveu uma análise abrangente dos fenômenos da natureza e da sociedade, conhecida como “Método de abordagem”; a segunda abordagem tratou dos procedimentos, a qual esclarece os “Procedimentos técnicos” utilizados (MARCONI; LAKATOS, 2003).

A forma como a abordagem foi conduzida para chegar às conclusões teve um caráter dedutivo, partindo das observações e de um conhecimento prévio baseado no repertório bibliográfico existente. A abordagem escolhida foi qualitativa, com ênfase na análise de

conteúdo, com o objetivo de interpretar e analisar o fenômeno observado a partir dos dados coletados.

Como procedimentos técnicos, a pesquisa bibliográfica foi realizada através da plataforma de busca no *Dimensions* AI, que é uma solução de busca e descoberta que integra os recursos de diversas instituições nacionais e internacionais. Neste portal, pode-se realizar uma pesquisa geral, pesquisando em todas as coleções disponibilizadas pelas instituições. Os termos (descritores) definidos para a pesquisa no motor de busca desta plataforma foram: {(("LGPD" OR "Lei Geral de Proteção de Dados") AND ("IoT" OR "Internet das Coisas")) OR (("GDPL" OR "*General Data Protection Law*") AND ("IoT" OR "*Internet of Things*"))} Estes descritores foram adotados após a realização de testes com outros termos com a finalidade de obtenção dos melhores resultados para o trabalho em questão. As opções de configuração selecionadas na plataforma definiram-se conforme apresentado no **Quadro 1**.

Quadro 1 – Configuração do mecanismo de busca pelo *Dimensions* AI

Tipo de Material:	Todos os tipos
Data de Publicação:	2019 a 2023
Idioma:	Qualquer Idioma
Busca em:	Título e Abstract

Fonte: Autoria Própria (2023).

Também ocorreu a definição de regras para segregação do material recuperado, sendo elas: "Alta relevância referente ao tema" e "Documento aborda os assuntos descritos do tema". A segregação se deu por meio das técnicas de leitura exploratória e seletiva no material coletado, para realizar uma segregação básica inicial. A seguir, foi utilizada a técnica de leitura analítica. E, por fim, ocorreu a leitura interpretativa, que nem sempre ocorre separadamente da leitura analítica, visando estabelecer uma relação entre o conteúdo das fontes pesquisadas e outros conhecimentos (GIL, 2002).

4 RESULTADOS E DISCUSSÃO

Após a aplicação do método, descrito na seção anterior, a plataforma forneceu dezesseis artigos, todos os artigos obtidos possuíam acesso aberto e foram analisados, seguindo um critério de dupla verificação, cujo resultado pode ser verificado no **Quadro 2**.

Quadro 2 – Lista de artigos e obtenção de resultados aderentes ao interesse da pesquisa

Título	Principais Evidências
Experimental Evaluation of a Checklist-Based Inspection Technique to Verify the Compliance of Software Systems with the Brazilian General Data Protection Law	O estudo avaliou a eficácia e eficiência da técnica para verificar a privacidade e proteção de dados em artefatos de software em comparação com técnicas ad hoc. Os resultados mostraram que a técnica de inspeção baseada em *checklist* é mais eficaz e eficiente do que as técnicas ad hoc para verificar a conformidade com a LGPD nesses artefatos. Além disso, o estudo identificou um conjunto de itens de verificação que podem ser usados para verificar a conformidade com a LGPD em artefatos de software, contribuindo para o desenvolvimento de novas tecnologias que garantam a qualidade do software sob a percepção de privacidade e proteção de dados pessoais.
Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal	O estudo avalia a efetividade e viabilidade do uso da técnica do uso de uma *checklist* (lista de controle) para avaliar se soluções de Internet das Coisas (IoT) se encontram adequadas a LGPD, tal *checklist* foi dividida em 3 categorias Segurança dos Dados, Segurança Física e Acesso ao Dispositivo, que se referem a proteção dos dados pessoais, proteção contra acesso físico aos dispositivos e variáveis de ambiente e controle de acesso ao dispositivo, respectivamente. A referida *checklist* foi aplicada em projeto de uma solução baseada em IoT para empresas industriais, onde dados pessoais e de dispositivos IoT são processados, após sua aplicação os participantes do projeto relataram que a *checklist* trouxe benefícios como identificar situações de segurança negligenciadas e encontrar facilmente falhas de segurança, o que mostrou que a *checklist* é capaz de identificar problemas reais no meio industrial.
Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados	O artigo discute a possibilidade de utilizar o *Personal Data Storage* (PDS) em conjunto com a Internet das Coisas (IoT) em conformidade com a LGPD. A proposta de PDS pode empoderar o usuário, dando maior controle e transparência sobre o tratamento de seus dados, e a IoT pode ser usada para coletar dados dos pacientes no Sistema Único de Saúde (SUS). No entanto, para que essa solução seja viável, é necessário resolver a aparente dificuldade da blockchain em ser certificada pela lei, os autores propõem uma solução teórica baseada em uma infraestrutura de PDS e na segurança da *blockchain*, mas reconhecem que ainda é necessário testar essa solução na prática.
Especificação de requisitos de design de software para sistemas de IoT conforme a LGPD: Resultados de aplicação em um sistema de assistência para pacientes com Diabetes Mellitus.	A pesquisa investiga e propõe uma abordagem de identificação análise e adequações de requisitos funcionais e não funcionais com a utilização de técnicas GORE (*Goal-Oriented Requirements Engineering* - Engenharia de Requisitos Baseada em Objetivos) e demais propostas para atender critérios da LGPD em sistemas IoT na saúde, e consequentemente, apoiar a etapa de design de software para que os sistemas de IoT possam se adequar às restrições de privacidade e segurança impostas pela legislação. A aplicação das diretrizes junto com as técnicas de GORE facilitou a identificação de todos os requisitos de conformidade de segurança e integridade dos dados propostas pela LGPD necessários para aplicação no cenário de estudo, que até então não propunha soluções para o tratamento de dados relacionados a legislação em seus requisitos funcionais e não funcionais. Como resultado foram identificados 25 requisitos funcionais divididos em 7 categorias e 16 requisitos não funcionais divididos em 5 categorias. Após a definição dos requisitos, 3 avaliadores foram selecionados para verificar a qualidade dos requisitos obtidos, O primeiro avaliador é advogado com especialização em privacidade de dados e é atuante na fiscalização na adequação dos sistemas de software a LGPD. O segundo avaliador é engenheiro de software com experiência na especificação de requisitos e uso do método GORE. O terceiro avaliador é especialista em IoT aplicada à saúde. Após o trabalho realizado pelos avaliadores é possível concluir que a especificação de requisitos realizada para adequar o sistema de IoT apresenta níveis razoáveis de qualidade, pois a maioria dos critérios foi avaliada com nota superior ou igual a 4, sendo os critérios: Corretude no uso do método de especificação de requisitos, completude dos requisitos, coerência com o domínio do sistema, coerência com a LGPD e clareza da descrição dos requisitos.

Fonte: Autoria Própria (2023).

Os estudos analisados convergem na eficácia e relevância do uso de *checklists* como ferramentas para verificar a conformidade com a LGPD em contextos de Internet das Coisas (IoT). A aplicação de *checklists* demonstrou ser mais eficaz e eficiente em comparação com abordagens ad hoc, proporcionando uma estrutura organizada para avaliar questões de segurança e privacidade.

A aplicação de *checklists* foi destacada em dois estudos específicos. No primeiro, a técnica de inspeção baseada em checklist demonstrou superioridade, identificando itens de verificação específicos e contribuindo para o desenvolvimento de tecnologias que garantem a qualidade do software, especialmente no que se refere à privacidade e proteção de dados pessoais.

Além disso, o LGPD *Check* incorpora em cada frame não apenas o princípio da LGPD, mas também sua interpretação específica para sistemas de software. Dentro de cada frame, são apresentados exemplos ilustrativos de violações e as ações esperadas dos proprietários do sistema ao conceber as atividades de processamento de dados, tudo alinhado com o princípio correspondente (André et al., 2023). Essa abordagem aprofundada reforça a importância dos *checklists* não apenas como ferramentas de avaliação, mas como guias abrangentes para garantir conformidade em todas as fases do ciclo de desenvolvimento de *software.*

No segundo estudo, um *checklist* dividido em categorias, como Segurança dos Dados, Segurança Física e Acesso ao Dispositivo, foi aplicada a projetos de IoT para empresas industriais.

Onde após a realização de um grupo focal com os participantes eles relataram que houve benefícios, destacando a capacidade da *checklist* de identificar situações de segurança negligenciadas e facilmente encontrar falhas de segurança. (PEREIRA et al., 2022).

Além da aplicação de *checklists*, um estudo explorou a integração do *Personal Data Storage* (PDS) com a Internet das Coisas (IoT) visando atender aos requisitos da Lei Geral de Proteção de Dados (LGPD). Essa iniciativa busca capacitar os usuários, proporcionando-lhes maior controle e transparência no gerenciamento de suas informações pessoais. Contudo, a efetiva implementação prática dessa solução ainda representa um desafio a ser enfrentado, especialmente no contexto da tecnologia blockchain. Destaca-se a importância da transição do modelo centrado no fornecedor de serviços para um enfoque centrado no usuário, conforme apontado pela evolução do Armazenamento de Dados Pessoais (PDS) e pela introdução do Regulamento Geral de Proteção de Dados (RGPD) (FALLATAH et al., 2023).

Outro estudo focou na identificação, análise e adequações de requisitos funcionais e não funcionais usando técnicas de Engenharia de Requisitos Baseada em Objetivos (GORE). Essa

abordagem buscou garantir que os sistemas IoT atendam aos critérios da LGPD, facilitou a identificação de todos os requisitos de conformidade de segurança e integridade dos dados propostos pela LGPD (RIBEIRO PEDRO; GARCÉS, 2023). Contribuindo para a etapa de design de software e promovendo a conformidade com as restrições de privacidade e segurança impostas pela legislação.

Ainda no âmbito da LGPD, um estudo explorou a legislação brasileira, destacando a abrangência da LGPD no tratamento de dados pessoais, independentemente do meio, país de sede ou localização dos dados. Essa consideração é crucial para organizações que operam em território nacional ou oferecem serviços a indivíduos nesse território.

Essa análise revela uma abordagem multifacetada para garantir a conformidade com a LGPD em contextos de IoT, abrangendo desde a utilização de *checklists* específicas até propostas teóricas, como o PDS, e a aplicação de técnicas de Engenharia de Requisitos. Cada abordagem oferece contribuições valiosas para promover a segurança, privacidade e conformidade legal em ambientes IoT.

Os resultados destacaram o *Personal Data Storage* (PDS) como um conjunto de capacidades em plataformas de *softwares* ou serviços, proporcionando aos indivíduos autonomia para gerenciar suas informações, artefatos e ativos digitais de forma autossuficiente (Fallatah et al., 2023). Essa abordagem representa uma proposta teórica destinada a reforçar o controle e a transparência no tratamento de dados sensíveis, especialmente no cenário da Internet das Coisas (IoT), pois sua implementação em sistemas informacionais complexos, que compartilham dados sensíveis, como os registros de saúde do SUS, ainda revela deficiências na preservação da privacidade dos usuários (AMÁLIA et al., 2021).

Aplicado em sistemas complexos, como o Sistema Único de Saúde (SUS), o PDS busca não apenas mitigar os riscos à privacidade dos usuários, mas também proporcionar-lhes maior autonomia sobre o acesso e uso de seus dados pessoais. A soberania dos dados, entendida como a capacidade dos indivíduos de controlar e determinar restrições sobre o uso de seus dados, destaca-se como um componente crucial do PDS (FALLATAH et al., 2023). O modelo enfatiza a necessidade de testes e abordagens práticas para avaliar sua eficácia em ambientes reais, reconhecendo desafios potenciais, como o aumento da responsabilidade para os indivíduos no gerenciamento de seus dados, especialmente aqueles sem experiência técnica (FALLATAH et al., 2023).

Além disso, o estudo que explorou a aplicação de técnicas de Engenharia de Requisitos Baseada em Objetivos (GORE) para identificar, analisar e adequar requisitos funcionais e não funcionais à LGPD oferece uma perspectiva centrada na qualidade e conformidade. A

participação de avaliadores com conhecimentos específicos, como um advogado especializado em privacidade de dados, um engenheiro de software experiente e um especialista em IoT aplicada à saúde, fortalece a qualidade dos requisitos obtidos.

A convergência entre os estudos reside na busca por soluções que assegurem a privacidade dos usuários, atendendo aos requisitos da LGPD em contextos diversos, desde artefatos de software até sistemas IoT aplicados à saúde. Essas abordagens refletem a necessidade crescente de incorporar considerações éticas e legais no desenvolvimento de tecnologias, especialmente aquelas que lidam com dados pessoais e sensíveis.

Esses resultados fornecem uma visão abrangente das estratégias adotadas para garantir a conformidade com a LGPD em ambientes de IoT, destacando a importância de abordagens específicas, como *checklists*, e propostas mais abrangentes, como o PDS, para promover a segurança e privacidade dos dados em conformidade com a legislação vigente. A continuidade desses estudos e a aplicação prática dessas abordagens são essenciais para avaliar sua eficácia em situações do mundo real.

5. CONSIDERAÇÕES FINAIS

O estudo explorou as interseções desafiadoras entre a Internet das Coisas (IoT) e a Lei Geral de Proteção de Dados (LGPD), buscando compreender as implicações, soluções e possíveis caminhos para a coexistência harmoniosa desses elementos.

Inicialmente, destaca-se o papel transformador da IoT, que redefine a interação humana com o ambiente, conectando dispositivos físicos e possibilitando tarefas antes inimagináveis. No entanto, à medida que a adoção de dispositivos e sistemas IoT cresce exponencialmente, surge uma preocupação crucial: a segurança e privacidade dos dados, especialmente quando se lida com vastas quantidades de informações pessoais e sensíveis.

A LGPD, um marco legislativo significativo, introduz uma mudança paradigmática no tratamento de dados pessoais, estabelecendo princípios que ressaltam a proteção de direitos fundamentais. No entanto, é observado que, embora a LGPD não aborde explicitamente a manipulação de dados em sistemas de IoT, a implementação de seus princípios pode preencher a lacuna regulatória existente. Nesse contexto, diversas abordagens foram exploradas, desde a eficácia de *checklists* na verificação de conformidade até a proposta teórica do *Personal Data Storage (PDS)* em conjunto com a IoT. A utilização de técnicas de Engenharia de Requisitos

Baseada em Objetivos (GORE) também se destacou, fornecendo diretrizes para adequar sistemas IoT às restrições de privacidade e segurança da LGPD.

Além disso, considera-se a aplicação prática do PDS em um contexto complexo, como o Sistema Único de Saúde (SUS), reconhecendo os desafios legais da blockchain e enfatizando a necessidade de testes na implementação real.

Conclui-se para a necessidade contínua de inovação e pesquisa prática para assegurar que a IoT e a LGPD possam coexistir de maneira eficiente. A harmonização desses elementos não apenas atende às exigências legais, mas também promove a confiança dos usuários, empoderando-se com maior controle sobre seus dados.

REFERÊNCIAS

ALBERTIN, A. L.; ALBERTIN, R. M. DE M. **A internet das coisas irá muito além das coisas.** GV EXECUTIVO, v. 16, n. 2, p. 13, 19 maio 2017.

ANDRÉ C., Diego; MAIANI, M. R.; HORTAT. G.. **Experimental Evaluation of a Checklist-Based Inspection Technique to Verify the Compliance of Software Systems with the Brazilian General Data Protection Law.** [S. l.: s. n.], 2023. Disponível em: https://doi.org/10.48550/arxiv.2308.14874. Acessado em: 24 nov. 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Lei no 13.709. Brasília, Brasil, 14 ago. 2019.

CAMARA, M. A. A.; LINS, G. H. A.; OLIVEIRA, F. H. C.; CAMELO, E. M. A.; MEDEIROS, N. R. F. C. **Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados.** Cadernos Ibero-Americanos de Direito Sanitário, vol. 10, no 1, p. 93–112, 18 mar. 2021. DOI 10.17566/ciads.v10i1.657. Disponível em: https://doi.org/10.17566/ciads.v9i3.657. Acessado em: 24 nov. 2023.

CAMARGO, P. A. L. **Lei geral de proteção de dados – LGPD e segurança na internet.** Revista Judicial Brasileira, vol. 3, p. 429–447, 27 Nov. 2023. DOI 10.54795/rejubesp.dirdig.232. Available at: https://doi.org/10.54795/rejubesp.dirdig.232. Accessed on: 17 Jan. 2024.

CHEN, S. et al. **A vision of IoT: Applications, challenges, and opportunities with China Perspective.** IEEE Internet of Things Journal. Institute of Electrical and Electronics Engineers Inc., 1 ago. 2014.

LIMA, A. A.; MAROSO, E. P. **LGPD-Lei Geral de Proteção de Dados: sua empresa está preparada?** Literare Books, 2020.

FALLATAH, Khalid U.; BARHAMGI, Mahmoud; PERERA, Charith. **Personal Data Stores (PDS): A Review.** Sensors, vol. 23, no 3, 1 fev. 2023. https://doi.org/10.3390/s23031477.

GIL, A. C. **A Pesquisa no Brasil: Promovendo a excelência.** 4. ed. São Paulo: Atlas, 2002.
KOHLS, C.; DUTRA, L. H.; WELTER, S. **LGPD: da teoria a implementação nas empresas.** SP: Rideel, 2021.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica.** 5 ed. São Paulo: Atlas, 2003.

PEREIRA, I.; MENDES, J.; VIANA, D.; RIVERO, L.; FERREIRA, W.; SOARES, S. **Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal.** Anais Estendidos do XIII Congresso Brasileiro de Software: Teoria e Prática (CBSoft Estendido 2022), , p. 28–31, 2022. Disponível em: https://doi.org/10.5753/cbsoft_estendido.2022.226679. Acessado em: 24 nov. 2023.

RIBEIRO P. J.; GARCÉS, L. **Especificação de requisitos de design de software para sistemas de IoT conforme a LGPD: Resultados de aplicação em um sistema de assistência para pacientes com Diabetes Mellitus.** Anais Estendidos do XXIII Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS 2023), , p. 37–42, 2023. Disponível em: https://doi.org/10.5753/sbcas_estendido.2023.229693. Acessado em: 24 nov. 2023.

WACHOWICZ, M. **Proteção de Dados Pessoais em Perspectiva–LGPD e RGPD na Ótica do Direito Comparado.** Curitiba, PR: Gedai, 2020.

ZEADALLY, S.; BADRA, M. (Ed.). **Privacy in a Digital, Networked World: Technologies, Implications and Solutions.** Springer, 2015.