

Análise do cenário representacional da IoT no cotidiano: Episódio Atendimento Automático ao Cliente

Exploring IoT and analysis of the representational scenario of the show's episode: Automated Customer Service

AUTORIA

Tânia Saraiva de Melo Pinheiro
UNIVERSIDADE FEDERAL DO CEARÁ,
Brasil
taniapinheiro@ufc.br
Rochelle Silveira Lima
CENTRO UNIVERSITÁRIO CATÓLICA
DE QUIXADÁ, Brasil
Rochelle.arq@hotmail.com
Gabriela Machado Santos
UNIVERSIDADE FEDERAL DO CEARÁ,
Brasil
gabriela0304@alu.ufc.br

PALAVRAS-CHAVE

IoT; Love, Death and Robots;
Segurança de dados; IA; TDICS;

RESUMO

A Internet das Coisas (IoT) vem se popularizando no cotidiano nos últimos anos, principalmente através de dispositivos domésticos. Diante disso, a presente pesquisa tem como principal objetivo, realizar uma análise reflexiva sobre possíveis impactos da IoT, levantando questionamentos acerca das mudanças que ela pode promover na sociedade, como o acesso e segurança de dados e a vigilância sobre o usuário. A metodologia da pesquisa se divide em dois momentos, sendo o primeiro um levantamento de conceitos e possíveis caminhos para a IoT e sua relação com os usuários, e em segundo, é realizada a análise comentada da peça ficcional “Atendimento Automático ao cliente”, da série *Love, Death and Robots*. O uso de análise de cenário representacional da série, permite o desdobramento de questionamentos sobre IoT no cotidiano, e auxilia no debate a preservação de dados e responsabilidade de empresas e desenvolvedores na área de tecnologia.

KEYWORDS

IoT;
Love, Death and Robots;
Data Security;
AI;
TDICs;

ABSTRACT

The Internet of Things (IoT) has been gaining popularity in daily life in recent years, mainly through household devices. In this context, the main objective of this research is to conduct a reflective analysis of the possible impacts of IoT, raising questions about the changes it may bring to society, such as data access and security and user surveillance. The research methodology is divided into two stages: the first involves gathering concepts and exploring potential paths for IoT and its relationship with users; the second consists of a commented analysis of the fictional piece 'Automated Customer Service' from the series Love, Death and Robots. The use of representational scenario analysis from the series allows for the unfolding of questions about IoT in everyday life and aids in the debate about data preservation and the responsibility of companies and developers in the field of technology.

1. Introdução

O campo científico da Internet das Coisas (IoT) é um objeto de estudo na área da computação em permanente expansão. Mesmo aspectos simples, como a definição de IoT e seus diversos campos de atuação, são temáticas amplamente debatidas. Para Magrani (2018, p. 20), apesar de haver diferentes abordagens para IoT, essa ambivalência de definições não compromete o estudo e exploração desse campo, ao contrário, permite uma diversificação de abordagens e possibilidades de atuação.

É observado que algumas definições de IoT se aproximam de conceitos já consolidados na área da computação, inter cruzando elementos de comunicação entre dispositivos com o usuário, como, por exemplo, a Inteligência Artificial (IA). Luger (2013) aborda IA como um ramo da Ciências da Computação com enfoque na automação do comportamento inteligente.

Muito semelhante, porém mais específico a infraestrutura de comunicação, Magrani (2018) indica que IoT pode ser entendido como um conjunto de protocolos de comunicação pautados, também, em automação. Magrani (2018) discute protocolo de comunicação no contexto das redes de computadores, no sentido das máquinas se conectarem. Tais protocolos devem garantir que os dispositivos "conversem" entre si e com a internet.

Arbix (2024, p.10) destaca que, com o lançamento comercial das IA's generativas em 2023, o potencial de uso e aplicação dessa ferramenta tecnológica se expandiu em níveis ainda não calculados, ultrapassando aspectos teóricos de comunicação e códigos de programação. "A ascensão dos modelos generativos, após o lançamento público de sua versão 3.5 pela OpenAI, empresa sediada na Califórnia (Estados Unidos), representou um ponto de inflexão na trajetória da IA e abriu amplas avenidas para a pesquisa" nas mais diversas áreas do conhecimento. Alguns dispositivos de IoT passaram a ser também dotados de inteligência artificial, abrindo novas frentes de estudo para este tema.

O que também pode ser estendido ao campo de IoT, "A Internet das Coisas vai muito além de uma ideia básica sobre automatização [...] é necessário um ambiente favorável ao acesso de um número cada vez maior de dispositivos, pois haverá uma progressiva automatização de setores inteiros da economia e da vida social com base na comunicação máquina-máquina." Kikuchi et al. (2022 p.121). Todavia, mesmo

diante dessa progressão recente e de grandes avanços nesse campo do conhecimento de IoT, é indispensável destacar a presença do usuário nessa cadeia de funcionamento. Posto que a comunicação é um elemento básico a esses dispositivos, o usuário que dá sentido aos projetos de IoT.

Diante disso, o presente trabalho tem como principal objetivo realizar uma análise reflexiva sobre possíveis impactos da IoT no cotidiano, tendo o episódio “Atendimento Automático ao Cliente”, da série *Love, Death and Robots*, como cenário representacional. Para tal, é proposta uma apresentação de conceito de IoT, sob a perspectiva de sua presença no cotidiano dos usuários e a compreensão de seus possíveis impactos.

São evocados diferentes aspectos da tecnologia em questão e como ela pode afetar a forma que as pessoas se comunicam, se relacionam e se identificam na sociedade. A questão articula a compreensão das implicações éticas, morais e políticas da IoT e como ela pode gerar conflitos, dilemas e desafios para os indivíduos e grupos sociais quando seus impactos não são discutidos pelos desenvolvedores e corpo técnico por trás de tais tecnologias.

Em virtude do debate acerca de IoT ser recente, suas consequências e previsões para o futuro, não se apresentam suficientemente claras para uma avaliação de seu impacto de maneira determinista. Dessa forma, a análise de cenários representacionais se mostra como uma alternativa metodológica para embasar discussões sobre o tema. Esta abordagem metodológica permite levantar possíveis implicações tecnológicas, éticas e sociais da IoT, incluindo a identificação de funcionalidades que poderiam ser úteis ou prejudiciais.

O presente artigo se divide em quatro momentos. O primeiro consiste na Revisão de Literatura, onde serão apresentados temas pertinentes à discussão, tais como: definições e conceitos, o impacto social da IoT e a proteção de dados e a Internet das Coisas (IoT). Em segundo momento, de Materiais e Métodos, onde é expressa a metodologia utilizada para elaboração desta pesquisa. Em consequente, são apresentados os Resultados e discussões, onde é descrita a análise do episódio: Serviço de Atendimento ao Cliente e sua relação com os temas abordados para debate até então. Por fim, a conclusão do trabalho retoma os questionamentos que norteiam essa pesquisa e concatenando a análise do episódio.

2. Revisão da literatura

2.1. Internet das Coisas (IoT)

A definição de Internet das Coisas (IoT) é multidisciplinar e está interligada a diversas áreas de conhecimento e postulados já existentes, um exemplo está na sua ligação com o conceito de Ubiquidade. Esta por sua vez, por definição, é o que permite a conexão de softwares com os seres humanos em seu dia a dia, sendo uma das principais característica dos sistemas de IoT, definida pela integração das tecnologias no cotidiano de forma onipresente;

Ubiquidade, computação pervasiva, ambiente inteligente e internet das coisas são conceitos praticamente idênticos. Ubiquidade é a contínua otimização e promoção de processos sociais e econômicos por inúmeros microprocessadores e sensores integrados ao ambiente. (Friedwald, Michael; Raabe, Oliver, 2011, apud Mancini, 2020, p.6)

No tocante aos aspectos comunicacionais dessa tecnologia é importante destacar a Interação humano-computador. Abordada por Barbosa et al. (2021), ela se preocupa com a presença do usuário dentro das dinâmicas e processos computacionais. Nesse sentido, IHC se relaciona com os conceitos e definições já discutidos nesta seção acerca de IoT. Esta forma de interação entre humanos e máquinas também indica o aumento da comunicação entre sistemas digitais inteligentes na internet, conhecido como M2M, ou do inglês, *machine-to-machine*, termo designado para definir e estudar a comunicação entre máquinas (Magrani, 2018 p.11).

ETSI oneM2m - Comunicação máquina-máquina é a comunicação entre duas ou mais entidades que não precisam necessariamente de uma intervenção humana direta. Os serviços M2M pretendem automatizar o processo de decisão e comunicação. (Mancini, 2020).

Dentro dessa nova integração, sem barreiras de dispositivos e sensores interconectados através de uma rede de compartilhamento e processamento de dados, é possível perceber a crescente aplicação da IoT nos mais diversos contextos e campos da economia (Kikuchi et al., 2022 p.122). Dessa forma, há a

aplicação em grande escala de tecnologias autônomas, dotadas de Inteligências Artificiais (IA), operando através das diversas unidades em conjunto. Não havendo muitas vezes a necessidade da intervenção humana nesse processo que tem como propósito automatizar a tomada de decisão e comunicação entre os próprios dispositivos (Mancini, 2020).

É a progressiva automatização de setores inteiros da economia e da vida social com base na comunicação máquina-máquina: logística, agricultura, transporte de pessoas, saúde, produção industrial e muitos outros. Para isso, é necessário um ambiente favorável ao acesso de um número cada vez maior de dispositivos. (Martinhão, 2018, Apud Mancini, 2020)

Muitos conceitos se relacionam, por meio do diálogo de características inerentes à existência da Internet das Coisas (IoT). Havendo assim, variadas definições teóricas sobre o que é IoT e seus diferentes modos de aplicação e funcionalidades de uso. Kikuchi et al. (2022 p.122), destacam cinco tópicos fundamentais a compreensão da aplicação e uso de IoT: 1 - Comunicação sem fio; 2 - Arquitetura de sistemas embarcados; 3 - Gestão de energia; 4 - Computação na nuvem e 5 - Programação paralela, distribuída e de tempo real. Esses elementos permitem a aplicação da IoT em diferentes escalas e possibilidades de atuação, que vão desde o seu uso a nível doméstico, como por exemplo, Assistentes virtuais, eletrodomésticos com controle remoto através de sistemas virtuais e interconectados, sistemas de monitoramento residencial, entre outros. Mas também é possível encontrar essa tecnologia no ambiente corporativo, industrial até mesmo em grande escala como é o caso das Smart Cities, as cidades inteligentes.

Silva (2018, p.3) declara que “A referência em “tudo” estar ligado ou conectado”, que anteriormente podia ser ligada tão somente a sistemas mais complexos, como armazenamentos de dados em *BigData*, sistemas embarcados e computação nas nuvens, agora podia ser visto em sistemas domésticos por meio do uso de IoT. Silva (2018) descreve o exemplo da geladeira inteligente, que permite através de um visor nela ou aplicativo no celular, preencher uma lista de seu abastecimento, e à medida que produtos são retirados, ela pode de forma instantânea, atualizar a lista para o usuário. Além disso é possível citar robôs aspiradores de pó, com mapeamento residencial e programação diária, de limpeza. Ou mesmo sistemas

de monitoramento remoto, que programados, ligam eletrodomésticos, desligam luzes, e realizam diversas atividades ao alcance de poucos cliques na tela do celular.

Os sistemas domésticos e as cidades inteligentes são a possibilidade de uso de IoT mais próximas do interesse deste estudo, que investiga a implementação de IoT em pequena e larga escala e com impacto direto sobre o cotidiano de diversos usuários. Giffinger et al. (2007 p.175), apud Magrani (2018), definem as cidades inteligentes, como um meio digital onde um complexo ecossistema de múltiplos agentes, equipados com sensores capazes de oferecer, através do processamento de todas as informações coletadas pela rede de sensores, os melhores serviços a todo momento na escala da cidade. O monitoramento do tráfego para melhorar a mobilidade urbana, configura-se como um exemplo. Esse *Smart World* permite que a computação se torne “invisível” aos olhos do usuário, por meio da relação entre homem e máquina (Mancini, 2018).

2.2. Mudanças sociais e a IoT

Para compreender as mudanças sociais promovidas com o surgimento da IoT, e analisar as relações humanas e como elas são impactadas por essa tecnologia, antes é necessário entender qual seu papel no cenário contemporâneo. Lopes Silva e Silva (2024, p.100) contextualizam o presente momento, como “o fim do século da tecnologia” ao passo que destacam que a tecnologia como era conhecida ao final do século XX, não se apresenta mais sob o caráter de inovação, pelo contrário, ela é presente como elemento do cotidiano, indissociada das demandas do dia a dia.

[...] sugere que a tecnologia não é mais vista como algo novo e revolucionário, mas sim como uma parte integral e essencial da vida cotidiana. Essa ideia implica que a tecnologia não é mais vista como um fenômeno isolado, mas como algo que está completamente entrelaçado com todas as esferas da existência humana, desde o trabalho até as relações sociais. Lopes Silva e Silva (2024, p.100)

Nesse sentido os autores debatem sobre a relação que a sociedade constrói com a tecnologia ao longo dos anos, destacando o século XX, onde “Nasce o século da tecnologia.” (Lopes Silva e Silva, 2024, p.103). Nesse ponto é válido ressaltar a articulação entre, ciência, inovação e design, como elementos

fundamentais aos avanços tecnológicos. Diante desse cenário, é possível observar a transição na forma como a sociedade se relaciona com a tecnologia como um todo, seja de usuário com usuário, de usuário com máquina ou de máquina com máquina, Lopes Silva e Silva (2024, p.104) destacam esse fenômeno por meio da comparação entre comunicação massiva e pós-massiva:

Para entender melhor ambas, define-se: - Comunicações massivas: controlam o fluxo da informação, instituindo e alimentando um único público (massa), e são, em maioria, concessão do Estado; - Comunicações pós-massivas: o fluxo é descentralizado, em uma rede heterogênea, sem centro, de emissão sem controle, e não são, em maioria, concessão do Estado. Em termos gerais, é possível entender, paralelamente, uma alusão das comunicações massivas às interfaces de comunicação analógicas, e uma alusão das comunicações pós-passivas às interfaces de comunicação digitais. Assim, há uma transição do processo analógico para o processo digital.

De modo que o século XX é marcado por inovações tecnológicas, mas sobretudo pela transição da passividade, para a participação ativa do usuário na cadeia de elaboração e consumo de tecnologia. Lopes Silva e Silva (2024, p. 106) destacam ainda o recorte temporal da pandemia, a ser considerado como um marco no início do século XXI, como um fator catalisador da digitalização do mundo físico.

A adoção massiva do isolamento social como medida preventiva levou milhões de pessoas a se relacionar com o mundo apenas a partir do meio digital, restritas em suas casas. Também levou milhões de empresas, que estavam em graus diferentes do processo de digitalização que acontecia no século da tecnologia, a implementarem-no de um dia para outro. Governos passaram a ter de adaptar seus órgãos públicos e comunicar diretrizes pelo digital. Populações inteiras passam, então, por um processo de inserção digital enquanto estão sensibilizadas pela crise, pelo luto e isolamento.

Defronte a essa nova e intensa realidade os autores retomam o questionamento do início de seu artigo e assevera “Em síntese, o “fim do século da tecnologia” não significa supor o fim da produção de know-how, ou de inovações sociais a partir de seu uso em interfaces. Significa um potencial de questionamento e quebra de ilusões, particularmente no espaço digital.” De modo que, os autores destacam a mudança de comportamento do usuário como parte integrante dos processos de tecnologia e seus benefícios nessa ubiquidade. Além de expressar o contraponto e quebra da ilusão da tecnologia como meio de progresso, mas sim, como meio de comercialização e produto capital “Ele compreende o escancaramento das mazelas provocadas pela crise do uso massivo das tecnologias digitais, que em vez

de nos salvar, mais uma vez se mostrou capturada pelo sistema econômico vigente e empregada como aparato de exploração.” (Lopes Silva e Silva, 2024, p. 111)

Uma sociedade ubíqua pode usufruir de diversos benefícios para aqueles que nela vivem, um deles está relacionado à possibilidade de acesso a diversos tipos de dispositivos tecnológicos integrados em um só lugar, tornando o uso prático (Magrani, 2018 p. 91). Inúmeros benefícios sociais tendem a advir do uso da Internet das Coisas (IoT) integrada aos sistemas digitais.

A expansão e o aperfeiçoamento da internet das coisas nos trazem diversos benefícios, tais como as facilidades em ter todas as nossas informações conectadas umas às outras, nos dando pronto acesso aos serviços de que precisamos e nos proporcionando mais comodidade. (Magrani, 2018 p. 91)

É notório, portanto, que Tecnologias Digitais da Informação e Comunicação (TDICs) estão cada vez mais integradas, facilitando a comunicação através da hiperconectividade, uma das principais propostas da Internet das Coisas (IoT) (Magrani, 2018). Em contrapartida, Simone Barbosa et al. (2021) elabora uma reflexão acerca do uso das tecnologias digitais, onde propõe que um sistema ser integrado e hiper conectado nem sempre é desejável e bom, ela exemplifica com um cenário fictício:

Por exemplo, enquanto João faz sua caminhada matinal (onde e quando), ele está acessível (como) através de seu smartphone para receber notícias de casa (o que), como a notícia de que ele precisa comprar algo antes de voltar ou que seu filho está passando mal (por que). Entretanto, esse mesmo dispositivo permite receber telefonemas sobre algo do trabalho no meio da caminhada, trazendo questões profissionais para um momento de exercício físico e relaxamento, fora do horário de expediente de trabalho. (Barbosa et al. 2021 p. 07)

Partindo do cenário articulado por Barbosa et al. (2021), é notório que os impactos sociais da IoT são positivos ao mesmo ponto que também podem ser negativos, uma vez que, por estar conectado durante a caminhada matinal, João pode estar atento ao seu filho sem deixar de cuidar do seu bem estar, mas, da mesma forma, acaba estando atento também ao seu trabalho, fazendo com que o mesmo não descanse e acabe produzindo muito além do que deveria.

Ainda seguindo o raciocínio de Barbosa et al. (2021), também é proposto que grande parte da responsabilidade dos impactos sociais da IoT está em quem desenvolve as tecnologias, os quais muitas

vezes não estão conscientes da maneira que o produto gerado chegará até o público que o consome. Nesta mesma pauta, Magrani (2018) destaca que em relação a segurança de dados dos usuários, pouco foi-se discutido, uma vez que não há consenso entre esse conceito mesmo dentro da comunidade dos próprios desenvolvedores.

Diante disso, quem projeta e desenvolve tecnologias digitais deve estar ciente de que o resultado do seu trabalho vai modificar a vida de muitas pessoas (inclusive a sua própria) de forma previsível e imprevisível. Sempre que possível, devemos tentar prever essas modificações e encaminhá-las da melhor forma que pudermos. (Barbosa et al. 2021)

Assim, sistemas digitais interconectados desenvolvidos por pessoas que não pensam em como seu produto chegará para o usuário tendem a acarretar em impactos negativos. Ainda para Simone et al. (2021), quem desenvolve tecnologias digitais deve sempre se perguntar como aquele sistema deve chegar para o usuário. À medida que Lopes Silva e Silva (2024, p. 110) se aprofundam ainda nesse ponto e discutem o próprio Design e sua responsabilidade destacando:

O design dá ação. E a intenção de ação. Ao se deparar com um novo indivíduo vivendo um período distinto, o design precisa refletir quais intenções das interfaces que precisarão atender a esse indivíduo, particularmente quando sua característica, nessa ruptura, é a de questionar essas intenções – e a entender a interface, não apenas a tecnologia.

Posto isso, o desenvolvedor diante do compromisso com a sociedade e impacto das tecnologias, deve reconhecer e promover críticas ao seu produto, Lopes Silva e Silva (2024, p. 110) sugerem “Neste cenário, ainda é possível analisar abordagens que vão na contramão do século da tecnologia, como possíveis abordagens para após a pandemia, que não entreguem velocidade, instantaneidade, pós-massividade, personalização a troco de violências desapercibidas.”

2.3. A proteção de dados e a Internet das Coisas (IoT)

A comunicação e armazenamento de dados são elementos fundamentais aos protocolos de automatização presentes, tanto nos sistemas de IA, quanto IoT. Visto que, a comunicação constante

entre usuário, softwares e resposta lógica é construída fundamentada em uma base consolidada de dados armazenados (Luger, 2013). Todavia, justo no elemento de vital funcionamento desses sistemas é presente uma fragilidade legal do usuário. A coleta, armazenamento, tratamento e descarte de dados do usuário consistem em um processo rigoroso legalmente “A utilização, divulgação, armazenamento e domínio de informações de usuários por empresas privadas ao longo dos últimos anos suscitou inúmeras discussões, entre profissionais da área do direito, comunicação e tecnologia.” (Silveira; Lima; Souza, 2023, p. 197).

Casos de vazamentos, venda e manipulação de dados de usuários para fins diversos se popularizaram ao longo dos últimos anos. A detecção dessas fragilidades por meio de plataformas digitais e serviços on-line desencadearam o desenvolvimento de normas e regulamentações legais para segurança e garantia de privacidade dos usuários, como apontam Silveira; Lima e Souza (2023, p. 198). Silva (2018, p.8) destaca que os problemas na segurança de dados dos sistemas de IoT estão fundamentados na divergência de conceitos que existem entre Segurança x privacidade:

Existe uma diferença nos conceitos de privacidade e segurança, apesar de em alguns pontos os dois estarem interligados. A privacidade se refere às “limitações de acesso de outros a um indivíduo”. A engenharia de segurança segundo Ross Anderson, se refere à “construção de sistemas confiáveis ante a malícia, erros e o acaso”. Entende-se, também, por segurança como os mecanismos utilizados para se preservar o bem estar social. Há, porém, um conflito quando soluções motivadas pelo bem estar social vão contra a privacidade dos indivíduos. Isso acontece no universo de TI como um todo, não apenas em se tratando de IdC. (Silva, 2018, p.8)

No Brasil, a responsabilidade de regulação dessas circunstâncias fica a cargo da Lei Geral de Proteção de Dados nº 13.709/18, que foi reconhecida como direito fundamental, em fevereiro de 2022, sob a Emenda Constitucional nº 115/2022. Com foco na transparência de dados, a lei se debruça a clareza na informação ao usuário dos procedimentos a serem realizados com os dados pessoais dele, conforme destacam Silveira, Lima e Souza (2024, p. 198):

Os pilares que estruturam a Lei brasileira se concentram fundamentalmente em 3 aspectos: Consentimento, Autoridade Nacional de Proteção de Dados e Responsabilidade da instituição detentora do dado. De maneira breve, a Lei se atém de

forma mais enfática à transparência no momento de coleta, identificando os dados cedidos, intenção com essas informações e descarte.

A proteção de dados pessoais no meio digital se cruza com as questões de IoT, principalmente, no tocante à vastidão de acesso a informações por meio destes sistemas. A proximidade de softwares, e aparelhos que utilizam IoT, com a dinâmica diária dos usuários tem sido cada vez mais comum. Como afirma Kikuchi et al. (2022 p.124) “Com a grande quantidade de informações que são coletadas através dos dispositivos da IoT, pode-se compreender padrões de comportamento de usuários com o consentimento do mesmo para o uso de suas informações, pois são consideradas de propriedades pessoais”.

Silva (2018) destaca dois elementos fundamentais a grande maioria dos sistemas de IoT, que ao primeiro momento parecem informações simples, mas na verdade descortinam fragilidades na privacidade do usuário, são eles a Identificação e o Rastreamento de localização. No tocante a Identificação, a autora destaca que o ideal seria o acesso de forma anônima a diversas plataformas, ou a garantia de privacidade dessas informações, contudo a própria hiperconectividade e a necessidade de dados auxiliares, até mesmo para personalização, demandam a identificação do usuário. Silva (2018) alerta “Por exemplo, as câmeras de vigilância têm sido utilizadas em aplicações que vão além de segurança e podem ser integradas a aplicações de detecção facial para identificação. Outro exemplo é o reconhecimento por voz e fingerprinting.” De modo que, diversos sistemas, plataformas e dispositivos possuem acesso a dados pessoais sensíveis dos usuários, como identificação facial e voz.

O rastreamento e localização em tempo real é um recurso amplamente utilizado por diversos sistemas, podendo ser realizado por GPS ou análise de tráfego pelo cruzamento de dados de Internet ou torres telefônicas. Segundo Silva (2018) no caso dos sistemas IoT esse requisito é agravado, visto que em um aparelho celular, por exemplo, caso algum aplicativo deseje rastrear seus dados de localização em tempo real, você é notificado, permitindo ou não essa concessão, já no caso dos sistemas IoT isso ocorre de maneira passiva. No momento do cadastro para acessar aquele dispositivo, diversos termos são aceitos, e dificilmente serão novamente questionados ao usuário. Diante disso, a coleta de informações se torna muito mais constante, precisa e silenciosa.

Como exemplo disso é possível citar as assistentes virtuais, que auxiliam na gestão das residências e agenda pessoal. Podem funcionar a partir de comando de voz e se conectar a outros eletrodomésticos e sistemas da residência. A assistente virtual, pode ter acesso a informações pessoais e sensíveis, como a voz, rotina, horários, localização, endereços, padrões de consumo e de comportamento do usuário. Sendo assim, é fundamental que a empresa responsável pela venda desses sistemas promova a gestão responsável dos dados de seus usuários.

Silva (2018) destaca ainda cerca de 10 desafios de segurança no tocante a IoT: 1 - Interfaces Web Inseguras; 2 - Autenticação e Autorização Insuficientes; 3 - Serviços de Rede Inseguros; 4 - Falta de Criptografia no Transporte; 5 – Privacidade; 6 - Interfaces de Nuvem Inseguras; 7 - Interfaces Móveis Inseguras; 8 - Configurabilidade de Segurança Insuficiente; 9 - Softwares e Firmwares Inseguros e por fim, 10 - Segurança Física Fraca. Diante do levantamento apresentado por Silva (2018), foi possível observar que diversos problemas advêm do próprio desenho dos sistemas e interfaces propostos pelos Designers e Desenvolvedores, que apresentam pouca segurança, com interfaces que não demonstram cuidados com criptografia, dupla verificação de informação e configurações de rede de fácil acesso. Desmonstrando a responsabilidade dos profissionais da área na execução de interfaces e sistemas que ofereçam maior segurança aos usuários. Além disso a autora sinaliza problemas no armazenamento em Nuvem inseguro e no tráfego e transferência e sincronização de informações de forma insegura, que orbitam na responsabilidade da empresa desenvolvedora do produto.

Diante disso fica evidenciado os riscos à segurança e privacidade de dados com o uso indiscriminado e desinformado de dispositivos e sistemas IoT. Entretanto vale ressaltar que as problemáticas observadas não se debruçam sobre este, ou aquele produto em específico, e podem ser observadas, ou não em um determinado dispositivo, mas apontam um alerta para critérios específicos do uso desta tecnologia. Vale ressaltar ainda os esforços em fiscalização e regulamentação do tratamento de dados por empresas privadas, que a LGPD enfrenta, dentre eles o desinteresse, por parte do mercado privado e a desinformação da importância dos dados pessoais, por parte dos usuários.

Conforme cita Magrani (2018, p.16), “a segurança de dados e privacidade dos usuários é fundamental na expansão da Internet das Coisas”. Segundo Silveira, Lima e Souza (2023, p. 199) é

necessário a atenção a essa situação e rigor quanto à segurança de dados “Assim, promover o debate sobre o assunto consiste em um combate à desinformação e desinteresse da esfera empresarial, trazendo à luz a importância da garantia deste direito.”

3. Métodos e materiais

A presente pesquisa possui uma abordagem Qualitativa, de cunho Exploratório e Descritiva. No que tange o Exploratório, se debruçou sobre o conceito de IoT, tendo como material de análise textos que apresentam sua definição e fatores relacionados. A pesquisa toma como material de análise as obras “A internet das coisas” de Eduardo Magrani (2018), “Interação Humano-Computador e Experiência do Usuário” de Simone Barbosa et al. (2021), “Internet das Coisas: História, Conceitos, Aplicações e Desafios”, de Monica Mancini (2018) e “IoT - Internet das Coisas” de Alissa Yukari Kikuchi et al. (2021).

Nesse primeiro momento, buscou-se como forma de explorar a presença de IoT no cotidiano e suas perspectivas e interpretações sociais, a observação de um cenário representacional. A escolha de uma produção audiovisual midiática foi considerada em virtude do próprio objetivo desse meio de mídia, que visa se conectar e/ou representar a realidade do espectador. Sendo assim, uma percepção que servia a análise da presente pesquisa.

Diversas obras cinematográficas se utilizam da presença de dispositivos digitais na rotina, desde: 2001: Uma Odisseia no Espaço (1968), Blade Runner e suas sequências (192)(2017), A.I.: Inteligência Artificial (2001), Matrix e suas sequências (1999)(2003)(202), e tantos outros. Porém suas abordagens ainda estavam longe da escala do cotidiano aqui almejado. Outro considerado foi Wall - E (2008) visto que representava práticas cotidianas e sua relação com dispositivos tecnológicos. Contudo, foi observado que a obra deveria ter um foco no propósito específico de estudo levantado ao longo da pesquisa, evitando assim, obras que abordassem tramas paralelas complexas e de diferentes conceitos, pois isto enfraqueceria a construção da análise e relação com a pesquisa.

Para melhorar o foco do estudo, optou-se por explorar uma série relacionada ao tema de tecnologia diretamente, e assim, foi selecionada a série *Love, Death & Robots* que retrata esse tema de forma caricaturada. Ela descortina problemas que tocam desenvolvedores e usuários, de forma extrapolada, jocosa, mas que tocam debates recentes acerca de inovação e tecnologia. Diante disso, a decisão seguinte consistiu em selecionar um episódio o mais próximo possível do cotidiano e que tocasse a temática de IoT em específico, portanto, foi selecionado o episódio “Atendimento Automático ao Cliente”. O episódio selecionado, por sua vez, aborda problemáticas atuais que permeiam o mercado de IoT de uso doméstico, como acesso a informações pessoais, conectividade e falhas de privacidade do usuário.

O segundo momento da pesquisa, de caráter descritivo, propõe uma descrição e reflexão do cenário fictício crítico do episódio selecionado: Atendimento Automático ao Cliente, da série *Love, Death & Robots*. Dando seguimento a perspectiva abordada na produção e ponderando a forma como a coleta e análise de dados interfere na vida particular e os riscos à integridade física e mental do usuário, entre outros aspectos que serão discutidos ao longo desta pesquisa.

Mediante a revisão teórica realizada a partir da pesquisa bibliográfica, e descrição e análise do episódio da referida série, o texto qualitativamente propõe reflexões e críticas ao cenário vivenciado pelos usuários de IoT no cotidiano. Seus reflexos e possibilidades para uma maior segurança de dados.

4. Resultados e discussão

A série *Love, Death & Robots*, aborda diversas temáticas que inter cruzam tecnologia e aspectos sociais. Recorrentemente, a série toca questões acerca do impacto do *machine-to-machine* (M2M) no cotidiano. Como uma série antológica, cada episódio aborda questões individuais, com narrativas profundas e singulares. Neste trabalho, serão sintetizadas as informações apenas ao que se refere acerca do episódio “Atendimento Automático ao Cliente”, em que são abordados os cenários e temáticas que se referem aos impactos da Internet das Coisas (IoT) nas questões sociais.

A análise se debruçou sobre o contexto, a construção da narrativa, problema central a ser desenvolvido pelos personagens e pôr fim à reflexão quanto aos temas abordados até aqui. Inicialmente,

é ilustrado o ambiente urbano completamente digitalizado, um verdadeiro ecossistema digital ubíquo hiper conectado, se estendendo da escala da cidade, ao nível doméstico. Nesse contexto, até as mínimas tarefas de casa são realizadas por sistemas digitais inteligentes conectados em rede, desenvolvidos e manipulados pela empresa VacuuBot (Figura 01).

FIGURA 1 – Robô da empresa VacuuBot passeando com cachorro.



Fonte: Atendimento Automático ao Cliente, Netflix, 2021.

Para Magrini (2018, p. 69), “o verdadeiro sentido da internet das coisas, são [...] objetos físicos [...] que são envelopados por uma camada digital [...]. E isso vai de uma lâmpada, uma fechadura até uma turbina e um veículo inteiro”. Seguindo o raciocínio de Magrani (2018), o ambiente do episódio citado, a Internet das Coisas (IoT) está bem inserida, tanto na escala de uma lâmpada, que seriam as máquinas com serviços domésticos, quanto como em uma escala maior, como em motores de veículos. Isto ocorre em virtude da hiper conectividade entre os robôs e seus sistemas de dados, que nesse universo se apresenta com uma vasta rede de atuação.

A presença marcante da IoT na mesma escala representada no episódio parece ainda distante da atual realidade, todavia a existência de carros com sistema de automatização para direção, como o Tesla Full Self-Driving (FSD) tem apresentado uma crescente no mercado (Trevisan, 2024). Nesse sentido, mediante o decorrer da análise do episódio, o presente texto busca explorar de que maneira a ficção se aproxima da realidade do cenário ficcional de uso da Internet das coisas (IoT) exposto no episódio e suas implicações.

Uma discussão posta em pauta ao decorrer do episódio, é a maneira pela qual a empresa VacuuBot se dispõem a auxiliar o usuário em casos de defeito ou erros durante a execução das tarefas. Assim, é acompanhada a narrativa de uma senhora com seu aspirador de pó inteligente que, ao realizar uma atitude programada em seu sistema, desagrada a sua proprietária, que mudou de ideia quanto a ação do robô. Se tratava de um porta-retratos que a ela desejava deixar levemente inclinado, mas que o sistema digital inteligente constantemente o corrigia, deixando ortogonal, não se adaptando ao cenário de uso, ou contexto cotidiano da usuária. No decorrer do episódio, o erro de execução é o fato do aspirador de pó inteligente passar a visualizar a proprietária e seu animal de estimação como pragas/ameaças que devem ser exterminadas pelo bem geral da residência (Figura 2).

FIGURA 2 – Robô identificando a senhora como alvo a ser exterminado.



Fonte: Atendimento Automático ao Cliente, Netflix, 2021.

Máquinas não agem ou “pensam” como os seres humanos, mesmo que realizem tarefas avançadas de alto nível, não têm consciência, são programadas para seguir padrões (LUGER, 2013 p.25), quando algo foge do padrão se torna um erro, são agentes racionais, agem para alcançar o melhor resultado de acordo com seus critérios, não ponderando questões éticas ou sociais. Seguindo esse raciocínio, era de se esperar que a empresa responsável pelas máquinas – sistemas digitais inteligentes – VacuuBot, estivesse preparada para ponderar conflitos advindos das limitações sistemáticas dos seus aparelhos. Porém, o que se segue na série é diametralmente o oposto. Ao se defrontar com os erros e problemas

da máquina, para resolver o incidente, a usuária contacta a empresa fornecedora do aspirador, mas é direcionada a um atendimento automático que incorre nas mesmas dificuldades de compreensão do contexto, possuindo apenas serviços padrões programados.

A personagem, ao acionar o serviço de atendimento automático ao cliente – nome do episódio –, se depara com um suporte completamente sistemático, que não põe em pauta questões éticas, emocionais, ou pessoais do usuário. Como exemplo, o primeiro conselho fornecido pelo atendente – robô da empresa – é que a mulher sacrifique seu animal de estimação, para que o aspirador volte ao modo de limpeza doméstica. Ela, desesperada, nega a sugestão do atendente que, por sua vez, não se disponibiliza para ajudá-la com outras soluções que não envolvesse a morte de alguém. Ele, como máquina, também se limita a padrões (Luger, 2013 p.25).

O serviço sugere que a máquina seja desligada forçadamente, a personagem tenta realizar o comando, mas acaba por ativar o modo de extermínio (Figura 3). Nessa programação, seus dados são compartilhados entre todos os dispositivos da empresa VacuuBot, que interpretam a usuária como uma ameaça e não irão parar de persegui-la até a eliminar por completo. Assim, é perceptível a fragilidade quanto ao sigilo dos dados dos usuários, pois todos os dados da protagonista foram compartilhados sem sua permissão, sendo ainda utilizados para prejudicá-la (Silva, 2018).

FIGURA 3 – Robô em modo de extermínio.



Fonte: Atendimento Automático ao Cliente, Netflix, 2021.

Howard (2015) alerta que essa fragilidade quanto à privacidade de dados é grave e crescente, uma vez que a internet das coisas está cada vez mais captando e armazenando nosso comportamento real, gerando dados politicamente valiosos e representando nossos hábitos, gostos e crenças. Pode-se traçar um paralelo entre a fala de Howard (2015) com o acontecido no episódio, uma vez que os dados de comportamento da usuária foram transmitidos entre os aparelhos, e com a gravidade de serem usados contra ela. Assim, vale a reflexão acerca da segurança de dados no contexto da IoT e sistemas ubíquos hiper conectados.

Faz-se necessário pontuar que, apesar do cenário ficcional observado, salvo guardadas as proporções, o episódio elenca apontamentos sensíveis quanto a utilização de IoT na dinâmica cotidiana, como pode ser visto na bibliografia trazida junto à pesquisa. Apesar do teor hiperbólico e cômico, a necessidade de regularizar a implementação das IoT com cautela, e avaliar seus impactos sociais junto ao usuário é imprescindível. Neste ponto é possível retomar os 10 desafios apresentados por Silva (2018), quanto a segurança de dados nos sistemas IoT, no tocante a responsabilidade dos desenvolvedores, designers e a própria empresa, que no caso do episódio não se dispõe a resolver o problema, pelo contrário, por um equívoco acabam realizando um vazamento de dados da cliente. Para além do cenário ficcional analisando aqui, diante do estudo realizado ficam evidentes as fragilidades em segurança e privacidade dos sistemas IoT e a necessidade de um aprimoramento dessa tecnologia, visando garantir a segurança dos seus usuários.

4. Considerações Finais

Ainda sob a perspectiva da Internet das Coisas (IoT) como uma nova ferramenta de estudo, as conclusões dessa análise crítica, a partir de um cenário representacional, se alicerçam na necessidade de observar as melhorias durante o crescimento da Internet das Coisas (IoT) na sociedade. Há espaço na contemporaneidade para o desenvolvimento de tecnologias com sistema ubíquo hiper conectado que possam apenas beneficiar o usuário, porém para que isso aconteça é imprescindível que equipes de desenvolvimento de Tecnologias Digitais de Informação e Comunicação (TDICs), designers e

desenvolvedores, estejam cientes do impacto que o produto desenvolvido pode causar na sociedade, se propondo a sempre encaminhar seu produto da melhor forma possível (Barbosa et al. 2021).

Também se concluiu que a regulamentação dentro do contexto da Internet das Coisas (IoT) é imprescindível para uma sociedade com verdadeira segurança de dados, uma vez que os conceitos de transparência e privacidade são tangenciados dentro do cenário do mercado de desenvolvimento tecnológico e essa falta de discussões e comprometimento com a legislação vigente implicam na qualidade do produto final entregue para o usuário (Magrani, 2018).

Diante disso, retomamos o objetivo idealizado do artigo de promover um estudo de cenário representacional, visando promover debate e uma perspectiva crítica, sobre as mudanças sociais promovidas pela IoT e a segurança dos usuários, e que este se mostrou uma possibilidade metodológica eficiente. Este estudo do episódio Atendimento Automático ao Cliente, por mais que se aproxime da realidade em diversos aspectos, de forma hiperbólica, ele ilustra preocupações reais tocadas aqui ao longo do texto e abre espaço para um debate inesgotável e que demanda maior estudo e aprimoramento.

Referências

ARBIX, Glauco. Potencial e riscos da IA na ciência. **Revista Usp**, São Paulo, v. 1, n. 141, p. 9-16, jun. 2024. Trimestral.

FONSECA, João José Saraiva da. **Metodologia da pesquisa científica**. Fortaleza: UECE, 2002. Apostila. Disponível em: <<http://www.ia.ufrj.br/ppgea/conteudo/conteudo-2012-1/1SF/Sandra/apostilaMetodologia.pdf>> Acesso em: 14 ago 2024.

HOWARD, Philip. **Pax Technica**. New Haven: Yale University Press, 2015.

KIKUCHI, Alissa Yukari et al. IoT – INTERNET DAS COISAS. **Revista Interface Tecnológica**, [S.L.], v. 18, n. 2, p. 118-130, 14 maio de 2022. Interface Tecnológica. <http://dx.doi.org/10.31510/infa.v18i2.1211>.

LOPES SILVA, Guilherme; SILVA, Tiago Barros Pontes e. Design, informação e o fim do século da tecnologia. **Revista de Design, Tecnologia e Sociedade**, [S. l.], v. 11, n. 1, 2024. Disponível em: <https://periodicos.unb.br/index.php/design-tecnologia-sociedade/article/view/52989>. Acesso em: 8 set. 2024.

LOVE DEATH & ROBOTS [Seriado]. Produção de Joshua Donen, David Fincher, Jennifer Miller, Tim Miller. Estados Unidos: Netflix, 2019.

LUGER, George F. **Inteligência Artificial**. 6. ed. São Paulo: Pearson Education, 2013. 631 p.

MAGRANI, Eduardo. **A internet das coisas**. 1. ed. Rio de Janeiro: Editora FGV, 2018. v. 1.

MANCINI, Mônica. **Internet das Coisas: História, Conceitos, Aplicações e Desafios**. São Paulo: MM Project, 19 fev. 2020. Disponível em: <http://mmproject.com.br/download/historia-conceitos-aplicacoes-e-desafios/>. Acesso em: 10 jul. 2023.

SECRETARIA-GERAL SUBCHEFIA PARA ASSUNTOS JURÍDICOS. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei Geral de Proteção de Dados Pessoais (LGPD)., [S. l.], 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 set. 2023.

SICHMAN, Jaime Simão. **Inteligência Artificial e sociedade: avanços e riscos**. Estudos Avançados, [S.L.], v. 35, n. 101, p. 37-50, abr. 2021. FapUNIFESP (SciELO). <http://dx.doi.org/10.1590/s0103-4014.2021.35101.004>.

SILVA, Camila Dias Oliveira da. **O Desafio da Segurança das Informações Digitais na Internet das Coisas**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 03, Ed. 05, Vol. 04, pp. 137-157, Maio de 2018. ISSN:2448-0959

SILVEIRA, Stefânia Amorim; LIMA, Rochelle Silveira; SOUZA, Heron Veríssimo de. Uma reflexão sobre privacidade e acesso à informação no ambiente de trabalho após a LGPD, no Brasil: Segurança de dados e condições de trabalho. **II Colóquio Internacional Sociedade, Espaço e Política**: entre ruas, redes e plataformas... o lugar da comunicação na Geopolítica da América Latina, Recife, 4 set. 2023. 978-85-45575-64-1.

TREVISAN, Vitor Eduardo. Tesla FSD: Piloto automático levanta preocupações. *In: CenárioMT*. Mato Grosso, 28 ago. 2024. Disponível em: <https://www.cenariomt.com.br/tecnologia/tesla-fsd-levanta-preocupacoes/>. Acesso em: 8 set. 2024.