UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

ENZO RAIAN TEIXEIRA CANDIDO

SEGURANÇA E PRIVACIDADE EM ASSISTENTES PESSOAIS

CAMPINA GRANDE - PB

2023

ENZO RAIAN TEIXEIRA CANDIDO

SEGURANÇA E PRIVACIDADE EM ASSISTENTES PESSOAIS

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Orientador: Professor Dr. José Antão Beltrão Moura.

CAMPINA GRANDE - PB

2023

ENZO RAIAN TEIXEIRA CANDIDO

SEGURANÇA E PRIVACIDADE EM ASSISTENTES PESSOAIS

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA:

Professor Dr. José Antão Beltrão Moura.

Orientador – UASC/CEEI/UFCG

Professor Dr. João Arthur Brunet Monteiro

Examinador – UASC/CEEI/UFCG

Trabalho aprovado em: 15 de Fevereiro de 2023.

CAMPINA GRANDE - PB

RESUMO (ABSTRACT)

In recent years, the automation of work and domestic activities has become indispensable for human beings, who are looking for ways to optimize time and get rid of repetitive and unwanted tasks. Personal assistants arrived to make life easier for these users, being driven by voice commands, they can, together with other devices, transform a common house into a smart home. However, as virtual assistants still have security and privacy flaws that can make their use dangerous, putting consumer data at risk. This work explores the main vulnerabilities present in virtual assistants and how the data of users who use this technology can be exposed, as well as investigating the perception of people regarding the leakage of their information.

Segurança e Privacidade em Assistentes Pessoais

Enzo Raian Teixeira Candido
enzo.candido@ccc.ufcg.edu.br
Universidade Federal de Campina Grande, Paraíba

José Antão Beltrão Moura
antao@computacao.ufcg.edu.br
Universidade Federal de Campina Grande, Paraíba

RESUMO

Nos últimos anos, a automação do trabalho e de atividades domésticas se tornou algo indispensável para os seres humanos, que buscam formas de otimizar tempo e se livrar de tarefas repetitivas e indesejadas. As assistentes pessoais chegaram para facilitar a vida desses usuários, sendo dirigidas por comandos de voz, elas podem juntamente com outros dispositivos, transformar uma casa comum em uma casa inteligente. Entretanto, as assistentes virtuais ainda possuem falhas de segurança e privacidade que podem tornar o seu uso perigoso, colocando em risco os dados dos consumidores. Este trabalho explora as principais vulnerabilidades presentes nas assistentes virtuais e como os dados dos usuários que utilizam essa tecnologia podem ser expostos, assim como investiga qual a percepção das pessoas quanto ao vazamento de suas informações.

Palavras-chave

Assistentes Virtuais, Segurança, Privacidade.

1. INTRODUÇÃO

Ao longo dos anos, a tecnologia vem evoluindo a passos largos, promovendo melhorias na qualidade de vida das pessoas, tornando o trabalho e as atividades domésticas mais fáceis e produtivas. As assistentes inteligentes resolvem diversos problemas presentes no dia a dia, fazendo com que atividades que antes eram repetitivas, possam ser realizadas através de um simples comando de voz. No âmbito doméstico, as assistentes pessoais combinadas com outros dispositivos de automação, podem transformar uma casa comum em uma casa inteligente, automatizando tarefas como acender e desligar luzes, tocar músicas, ligar aparelhos como cafeteiras, microondas, televisão, criar lembretes na agenda ou qualquer dispositivo que esteja integrado a ela. Além disso, elas são muito utilizadas para comandar câmeras e fechaduras inteligentes que garantem uma maior segurança para residências. Sendo possível ter uma casa totalmente integrada que recebe e executa ordens até mesmo na ausência de moradores.

Devido aos benefícios e a sua facilidade de uso, os dispositivos inteligentes vêm se mostrando em crescente ascensão. Pesquisas feitas pela think thank Pew Research Center, apontam que cerca de 21% da população dos Estados Unidos possuem pelo menos um alto-falante inteligente [1], e 85% dos adultos possuem um smartphone, no qual geralmente está incluso um software com assistente pessoal como Alexa, Siri ou Google Home [2].

Estes dispositivos funcionam através da voz do utilizador e têm como objetivo realizar as várias tarefas que lhe forem pedidas, tais como, comprar bens e alimentos, gerir listas de tarefas, responder a perguntas que envolvam conhecimento, tocar música, planear férias, controlar outros dispositivos domésticos inteligentes, enviar mensagens, fazer chamadas e muitas outras atividades. [3]

O que muitos não sabem é que os alto-falantes inteligentes são capazes de monitorar e entender a fala dos seus usuários e através da detecção acústica eles conseguem informações sobre o que a pessoa está fazendo, em qual cômodo ou local ela está inserida no momento e até mesmo dados de consumo que posteriormente podem ser negociados para grandes empresas que querem anunciar para seus consumidores. Em abril de 2019, a Amazon admitiu que as gravações de voz dos seus consumidores são ouvidas regularmente com o objetivo de melhorar o seu serviço [4]. A gigante de tecnologia Google também afirmou em julho de 2019, que os contratantes escutam regularmente as gravações de voz obtidas pelo Google Home [5]. Desse modo, é possível constatar que as empresas que vendem esses aparelhos de voz muitas vezes utilizam os dados sigilosos dos seus consumidores sem permissão para beneficiá-las.

Diante do exposto, o presente trabalho tem como objetivo expor as principais vulnerabilidades presentes em assistentes virtuais, bem como problemas na autenticação de voz, detecção acústica pelos contratantes, direito de privacidade de conversas gravadas e injeção de voz sem a consciência do usuário. Ademais, será feita uma pesquisa com os usuários de assistentes pessoais com o intuito de verificar a percepção dos mesmos quanto às vulnerabilidades apresentadas acima e os possíveis vazamentos de dados sigilosos face às falhas presentes nesses dispositivos.

2. TRABALHOS RELACIONADOS

Ultimamente, uma série de artigos publicados em sites de notícias e periódicos, vem trazendo a questão de segurança e privacidade em assistentes pessoais, tornando o tema relevante para um público maior.

Foram selecionados dois artigos a partir de alguns critérios além da relação com a pesquisa, o impact factor elevado do periódico onde o trabalho foi publicado, Proceedings of the IEEE com IF de 14.91, e ainda a quantidade de citações, sendo que os estudos foram citados por 5 autores acadêmicos.

Há uma recolha de dados pessoais e comunicações de voz dos utilizadores através desses dispositivos, dados que podem ter sido gravados em espaços privados, já que os dispositivos se encontram nas residências dos utilizadores. Esta recolha de dados, pode traduzir-se numa gravação de conversas do utilizador sem a sua permissão ou conhecimento. Isto pode acontecer devido ao fato dos aparelhos dos dispositivos de assistência virtual estarem ligados a internet e os dados serem armazenados na cloud, havendo por isso um maior risco de ciberataque ou falha mecânica [6,7].

Cheng & Roedig (2022) em seu trabalho citam quatro categorias de falhas presentes, duas relacionadas ao termo segurança e outras duas referentes ao termo privacidade, são elas [8]:

- Ataques através do canal acústico que tentam burlar a autenticação de voz, comprometendo o controle de acesso, permitindo que o invasor tenha acesso aos dados e que consiga interagir com os serviços disponibilizados pelos dispositivos. Um exemplo aqui é a injeção de comandos de voz, que geralmente são realizados através de sons inaudíveis pelos seres humanos, mas que são reconhecidos pelas assistentes.
- Ataques DDOS acústicos que podem desativar a interface de voz temporariamente, tornando indisponível serviços para os usuários. Um exemplo aqui é a interferência acústica, que tem como alvo a identificação da palavra de ativação do dispositivo.
- A utilização dos dados de voz dos usuários pelas grandes empresas que geralmente escutam a gravação das conversas dos seus consumidores sem o seu consentimento, o que pode levar a uma perda de privacidade, visto que informações confidenciais das pessoas podem ser vazadas.
- Uso de sons presentes no ambiente, não focados no processamento da voz corrente, que podem trazer informações relevantes sobre o ambiente que o usuário se encontra e que podem acabar revelando informações pessoais da localização do consumidor.

O artigo intitulado “A Survey on Voice Assistant Security: Attacks and Countermeasures” [9] elencou métodos de ataques existentes que podem pôr em risco a segurança dos usuários de assistentes pessoais, executando comportamentos maliciosos sem a permissão do proprietário. O trabalho destaca seis categorias de ataques, que são separados principalmente pela percepção humana, são eles:

- Uso da fala normal do invasor ou uma voz gerada por um software de conversão de texto em fala.
- Falsificação da voz que tenta imitar a voz do proprietário da assistente pessoal.
- Utilização de fala ininteligível pelos humanos, na tentativa de ocultar a intenção maliciosa. Estes sons geralmente são estranhos na vida real e podem levantar suspeitas do usuário.
- Utilização de sons especificamente projetados que parecem normais e benignos para o usuário, mas que são ataques maliciosos mascarados.
- Uso de sons inaudíveis para humanos, como ultra som, luz e ondas eletromagnéticas como portadoras para injetar comandos maliciosos.
- O invasor pode esperar que o proprietário pronuncie um comando que desencadeia involuntariamente uma habilidade maliciosa de terceiros, que podem ser serviços estendidos como as habilidades que podem ser instaladas em assistentes.

Os artigos acima indicaram pontos relevantes, mostrando vulnerabilidades em assistentes pessoais que muitas vezes passam despercebidas pelos usuários e até mesmo por desenvolvedores experientes da área de TI. Saber quais são elas e como são desencadeadas é de extrema importância para prevenção desses ataques.

Outro aspecto importante no campo dos desafios da privacidade é a falta de conscientização dos usuários em relação aos potenciais perigos que o uso de assistentes virtuais acarreta, assim como, uma falta de conhecimento em relação ao uso dos seus dados em diferentes contextos. Isto sucede, porque muitas vezes as empresas não são transparentes na forma como recolhem e armazenam os dados dos seus clientes. Como consequência, poderá crescer a falta de confiança dos utilizadores nas empresas que comercializam este tipo de serviço e dispositivos [6,7,10].

3. METODOLOGIA

Para atender ao objetivo desta pesquisa, foi realizado uma survey (obtenção de informações quantitativas), com o intuito de coletar opiniões dos participantes acerca da sua percepção quanto ao vazamento de dados face às vulnerabilidades e falhas presentes em assistentes pessoais. A survey foi criada utilizando o Google Forms e enviada

em vários canais de comunicação. Teve como público alvo: alunos de graduação de Ciência da Computação da Universidade Federal de Campina Grande, podendo ou não ser usuários de assistentes virtuais.

O questionário ficou disponível por 1 mês, entre o período de 10/12/2022 a 10/01/2023. A pesquisa foi formulada com o intuito de diagnosticar quais assistentes pessoais são mais utilizados, como elas são usadas e principalmente se os usuários estão cientes dos riscos e vulnerabilidades presentes nesses dispositivos. Desse modo, o questionário segue dois percursos, um para os casos em que o entrevistado responde que não usa assistentes pessoais nas duas primeiras perguntas e o outro, destinados aos usuários que utilizam os aparelhos e que continuarão respondendo a pesquisa.

A Survey contém 10 perguntas, das quais 7 delas ficam disponíveis apenas para pessoas que utilizam ou já utilizaram as assistentes pessoais físicas ou virtuais. O questionário obteve 81 respostas, que em seguida foram exportadas para um CSV, assim sendo possível realizar uma análise destes dados utilizando a linguagem Python juntamente com a biblioteca Pandas.

4. RESULTADOS OBTIDOS

Esta seção juntamente com suas subseções tem como objetivo apresentar e discutir os resultados obtidos na survey. As subseções foram separadas da seguinte forma: Primeiramente é mostrado o perfil dos entrevistados (4.1), posteriormente, a subsecção 4.2 mostra uma distribuição geral do uso das assistentes inteligentes, mostrando quais são mais utilizadas e quais foram abrangidas na pesquisa. Enquanto que a subseção 4.3 discute os resultados obtidos.

4.1. PERFIL DOS ENTREVISTADOS

A ideia deste trabalho é avaliar qual a percepção dos usuários quanto ao vazamento de seus dados em face de vulnerabilidades e falhas em assistentes pessoais. Desse modo, foram obtidas respostas de 81 respondentes, sendo 72 usuários de assistentes pessoais que cursam Ciência da Computação na UFCG (Universidade Federal de Campina Grande) de diversos períodos de ingressão. Todos eles possuem o entendimento mínimo do que é uma assistente pessoal e para que funciona, e a maioria deles já utilizou um desses dispositivos pelo menos uma vez.

4.2. UTILIZAÇÃO DE ASSISTENTES PESSOAIS PELOS RESPONDENTES

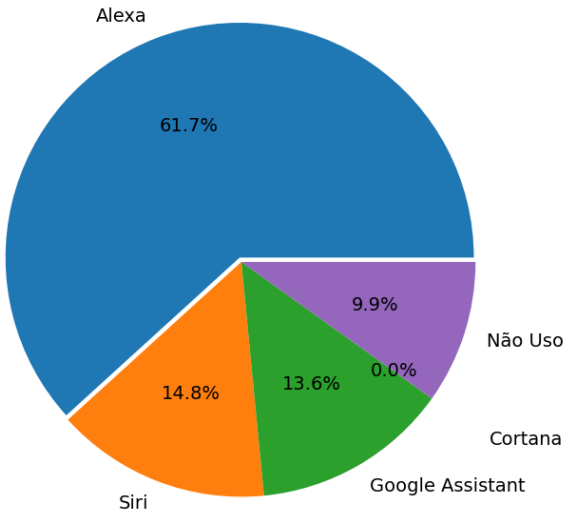
Na tabela 1 estão as assistentes pessoais físicas e virtuais exploradas na pesquisa e suas respectivas empresas.

Tabela 1: Dispositivos explorados na pesquisa com suas respectivas empresas.

Empresa	Assistente Pessoal (Nomes)	Dispositivos presentes
Amazon	Alexa	Echo, Echo dot
Apple	Siri	Iphone, Ipad, Mac
Google	Google Now e Google	Google Home e qualquer celular com Sistema Operacional Android.
Microsoft	Cortana	Qualquer computador com Sistema Operacional Windows.

Através da pesquisa foi constatado que a assistente pessoal Alexa da Amazon, é a mais utilizada pelos usuários da pesquisa, usada por cerca de 61.7% dos entrevistados, seguida da Siri da Apple, com 14.8%, Google Assistant, da Google com 13.6%, Cortana da Microsoft com 0%, sendo que 9.9% dos entrevistados não utilizam nenhum dispositivo. Outrossim, o trabalho mostrou que existe uma adesão forte pela utilização desses aparelhos, visto que aproximadamente 90% das pessoas consultadas utilizam algum assistente de voz.

Figura 1: Uso de Assistentes Pessoais pelos entrevistados

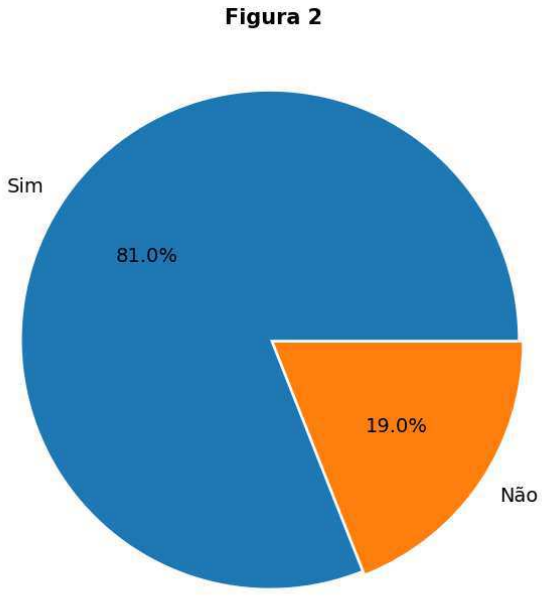


4.3. SEGURANÇA DAS ASSISTENTES PESSOAIS

Nesta seção foram realizadas perguntas relacionadas a segurança das assistentes pessoais, verificando qual a percepção dos usuários através de suas respostas.

Com relação à segurança de uma assistente pessoal, você acredita que há chance de algum vazamento de seus dados pessoais?

Figura 2: Chance de algum vazamento de seus dados pessoais



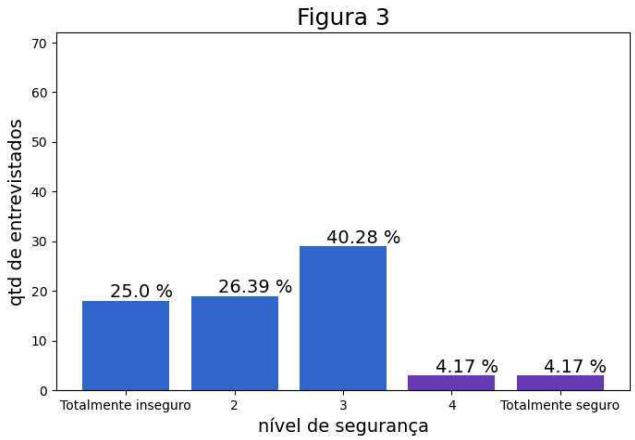
Constatamos que muitos consumidores desconhecem os riscos das assistentes pessoais, visto que quase 20% dos entrevistados na pesquisa acreditam que os seus dados pessoais não podem ser expostos por causa das vulnerabilidades presentes nesses dispositivos. Esta informação é preocupante, uma vez que já foi comprovado que os dados podem ser vazados de diversas formas e concluímos através dessas respostas, que uma parcela significativa dos seus utilizadores não têm sequer consciência dessa informação.

Você se sente seguro em saber que qualquer pessoa que fale a palavra de ativação de sua Assistente Virtual, têm acesso a suas informações pessoais como: agenda, lembretes, lista de contatos e despertador?

Todas as assistentes pessoais vem configuradas de fábrica com uma palavra de ativação que deve ser pronunciada para acionar o dispositivo, os aparelhos da Amazon são acionados pela palavra "Alexa", os da Google utilizam "Ok, Google", os da Apple "Ei, Siri" e os da Microsoft utilizam o comando "Ei, Cortana". Por padrão, qualquer pessoa que falar o termo de ativação consegue modificar todas as informações presentes nos dispositivos.

Muitas pessoas utilizam assistentes pessoais para criar lembretes, temporizadores utilizando a técnica pomodoro (parar e descansar) e uma agenda para não perder nenhum dos seus compromissos. O acesso dessas informações por terceiros mal-intencionados podem modificar os dados e acarretar sérios danos como a exclusão de contatos importantes, desmarcação de lembretes e de rotinas diárias, que são capazes de fazer com que o usuário perca compromissos importantes como reuniões e a ingestão de medicamentos importantes para sua saúde.

Figura 3: Segurança com relação à palavra de ativação da Assistente Virtual

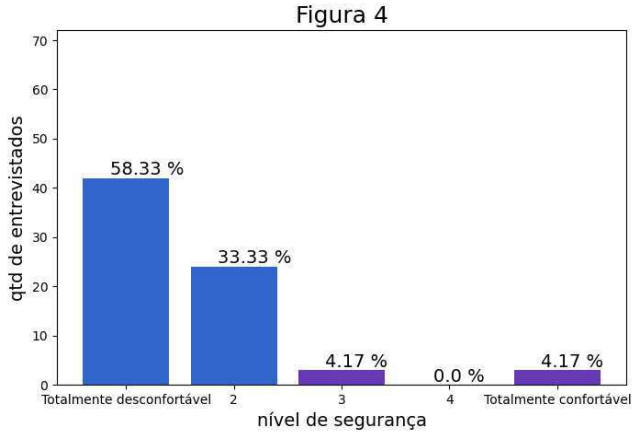


De acordo com os respondentes, 40.28% afirmaram ter um nível moderado a essa pergunta, conforme Figura 2, o que se mostra um dado alarmante, já que se tratam de informações sensíveis. Entretanto, devemos considerar também que alguns usuários utilizam assistentes pessoais apenas para ouvir música e podem não usar as habilidades como: agenda e lembretes, estando assim mais seguros com relação a esse risco.

O quanto você se sente confortável sabendo que suas informações podem ser alteradas por terceiros?

Por meio de uma escala likert, podemos observar na Figura 3 que há quase uma unanimidade entre os entrevistados, visto que cerca de 91% (Totalmente desconfortável e desconfortável) das respostas mostram que os consumidores não se sentem confortáveis sabendo que suas informações podem ser modificadas por terceiros.

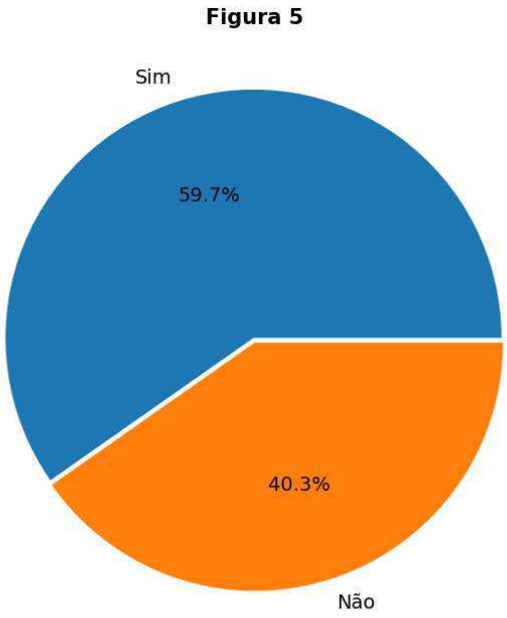
Figura 4: Conforto com relação a informações que podem ser alteradas por terceiros



Você permitiria uma empresa usar suas informações pessoais para treinar inteligência artificial usada em assistentes pessoais?

Conforme a figura 5, 59.7% dos respondentes estão de acordo com a utilização dos seus dados pelas empresas para treinar a inteligência utilizada nos dispositivos, enquanto 40.3% não estão de acordo com esse uso.

Figura 5: Permissão para uma empresa usar informações pessoais para treinar inteligência artificial usada em assistentes pessoais

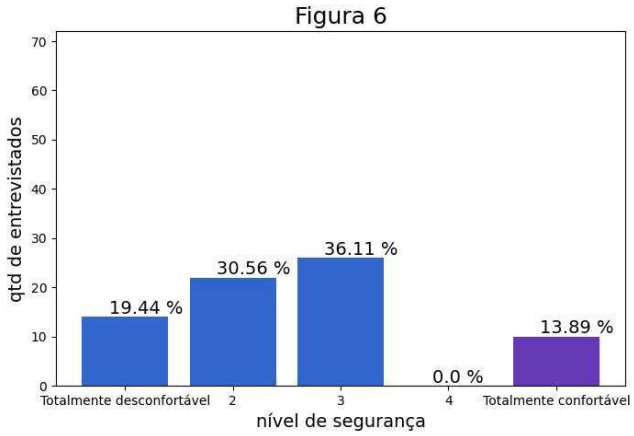


Existem pontos positivos e negativos na utilização desses dados dos usuários por parte das empresas. Através do tratamento e da análise dessas informações, as companhias que vendem esses dispositivos conseguem treinar a inteligência artificial utilizada neles com o uso de aprendizagem de máquina, promovendo uma melhoria nos seus serviços e uma melhor experiência ao consumidor. No entanto, liberar os dados de forma irrestrita para as empresas pode ocasionar sérias consequências, como a violação de privacidade, escuta e vazamento de conversas sigilosas, venda de dados para outras empresas que anunciam de forma online, sem a aprovação e consentimento do cliente.

Você se sente confortável falando assuntos sigilosos próximos a uma assistente pessoal?

A figura 6 apresenta respostas preocupantes por parte dos usuários, uma vez que na escala moderada temos 36.11% e na área de totalmente confortável que abrange 13.89% dos entrevistados que demonstram desconhecer o que as grandes corporações fazem com seus dados.

Figura 6: Sensação de conforto quando se fala em assuntos sigilosos próximos a uma assistente pessoal

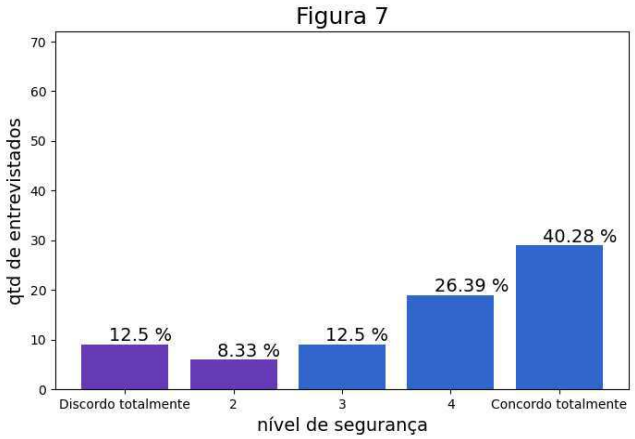


Essa preocupação é plausível pelo fato que ex-funcionários de grandes empresas que produzem assistentes pessoais, confessaram que ouviram conversas íntimas de casais e criminosos negociando drogas, gravadas inadvertidamente pelos dispositivos. Além disso, as próprias empresas admitiram que escutam gravações de voz dos usuários regularmente com o intuito de melhorar seus produtos e serviços [4].

Você acredita que a configuração para a assistente pessoal reconhecer apenas a fala do proprietário pode garantir maior segurança ao usuário?

Como podemos observar na Figura 6, 40.28% dos respondentes afirmam concordar totalmente que assistente pessoal reconhecer apenas a voz do proprietário pode garantir uma maior segurança. De fato, essa funcionalidade pode garantir uma maior segurança para os dados dos usuários, mas ainda assim existem diversas estratégias de ataques através do canal acústico que podem burlar a autenticação de voz, comprometendo o controle de acesso do sistema. Nessa situação, outras técnicas podem ser adotadas para garantir uma maior segurança aos dados de cada usuário, dentre elas podemos citar a remoção de configurações padrões de distribuição de dados, que as empresas de tecnologia incorporam fortemente nos seus dispositivos e que normalmente nos fazem compartilhar informações sobre nossas atividades e localização.

Figura 7: Configuração para a assistente pessoal reconhecer apenas a fala do proprietário pode garantir maior segurança ao usuário



No presente momento, a Amazon possui um hub de privacidade da Alexa, onde traz uma explicação completa sobre os tipos de dados coletados e como alterar suas configurações de privacidade, através de funções como a desativação de verificação humana, exclusão do histórico de gravações de voz e a utilização de um botão que desativa o microfone quando estiver tendo conversas delicadas, conseguimos garantir uma maior segurança a esse dispositivo. A Siri, é um dos que mais necessita de melhorias com relação a seus controles de privacidade, não existe a possibilidade do usuário revisar as gravações da Siri associadas a sua conta, dessa forma, a única solução presente até o momento é desativar a assistente totalmente do seu aparelho, fazendo assim com que seus dados dos servidores da Apple sejam removidos e quando quiser utilizá-la novamente, será necessário realizar a reativação. Já a Google Assistant, permite a desativação de revisões humanas e a exclusão das solicitações feitas pela assistente após um certo período de tempo, mas não possui um hub de privacidade explicativo como o da Amazon [11].

5. PROCEDIMENTOS E PRECAUÇÕES PARA REDUÇÃO DE RISCOS

A privacidade de assistentes pessoais têm cada vez mais importância e com isso terá que ser feito um grande investimento por parte dos países e das empresas em formas de proteger as informações e dados partilhados através desses dispositivos. As leis, melhores práticas regulamentações em vigor, se seguidas, podem impactar muito positivamente a segurança da informação dos dispositivos.

Como faz o Inmetro em suas áreas de atuação, essa entidade emitiria um selo, e para recebê-lo, os fabricantes teriam que seguir à risca as melhores práticas, que estipulariam um patamar mínimo de segurança para os dispositivos. As penalidades seriam aplicadas aos fabricantes e desenvolvedores que, caso não seguissem as melhores práticas, tivessem incidentes de segurança envolvendo seus produtos. A comunicação dos incidentes também é de suma importância, ela iria alertar os usuários dos dispositivos sobre as falhas,além de orientá-los sobre como mitigar o problema, seja com uma simples alteração de senha ou com atualizações de software fornecidas pelos fabricantes [12].

Atualmente, somente os criminosos que se aproveitam dessas falhas são punidos, mas fabricantes de dispositivos que não oferecem requisitos mínimos de segurança em seus produtos também devem ser responsabilizados. No mundo da cibersegurança é impossível chegar ao ponto de estar 100% seguro, por isso, se o fabricante ou desenvolvedor segue as leis e melhores práticas de segurança, não há por que eles serem punidos [12].

6. CONCLUSÃO E TRABALHOS FUTUROS

O presente trabalho teve como objetivo entender como funcionam as assistentes pessoais e como elas são utilizadas, com ênfase na percepção dos seus usuários acerca do vazamento de seus dados em face das vulnerabilidades e falhas presentes nesses dispositivos. Para esse fim, foi enviada uma survey para alunos de Ciência da Computação da Universidade Federal de Campina Grande, dos quais a maioria usa algum assistente inteligente. Com o questionário foi possível coletar informações importantes acerca do tema para realizar a análise proposta pelo estudo. Dessa forma, o trabalho contribuiu como um alerta aos usuários desses dispositivos, não só aos respondentes da pesquisa, mas como também os leitores deste artigo, visto que mostrou várias vulnerabilidades presentes nas assistentes virtuais e

também soluções para mitigar os riscos presentes nesses dispositivos.

A porcentagem de participantes que utilizam alguma assistente pessoal se mostrou alta (90%), demonstrando que esses dispositivos são largamente utilizados pelos cientistas da computação. A empresa Amazon engloba cerca de 62% dos entrevistados, que utilizam a sua assistente pessoal Alexa, que atualmente é a que concentra a maior parcela do mercado, em diferentes dispositivos presentes em smart tvs, smartphones e alto-falantes.

Concernente a segurança desses dispositivos, os participantes não demonstram estar cientes dos seus reais riscos de vazamento de dados. A maioria dos levantamentos feitos por parte da mídia e dos usuários estão concentrados na área de privacidade do utilizador. Esse é um ponto importante que deve ser pensado e, ao mesmo tempo, formular leis que evitem com que as grandes corporações tenham acesso aos dados de forma irrestrita como ocorre atualmente.

Entretanto, o que chama atenção na pesquisa é que os usuários de assistentes inteligentes não compreendem o risco principal explorado por agentes maliciosos, considerando que 19% dos entrevistados não acreditam que seus dados pessoais possam ser vazados de alguma forma.

Os resultados obtidos nessa pesquisa não podem ser generalizados, devido ao tamanho da população que foi investigada e para quais usuários foram destinados, desse modo, é pertinente refazer o estudo com diferentes públicos alvos, dentre eles usuários iniciantes em relação ao entendimento de tecnologia.

6.1 SUGESTÃO TRABALHOS FUTUROS

Dada a complexidade e pertinência do trabalho, sugere-se a continuidade com as seguintes sugestões:

- Replicar o trabalho explorando outras parcelas da população, para adicionar com os resultados obtidos nessa pesquisa e torná-los mais precisos.
- Outras questões poderiam ser elaboradas sobre quais funcionalidades das assistentes virtuais são mais utilizadas pelos respondentes, para assim entender a quais riscos eles estão expostos.

AGRADECIMENTOS

Agradeço primeiramente ao Professor Dr. José Antão por toda a sua dedicação e apoio, sua presença foi imprescindível para execução deste trabalho. A minha família que me apoia na faculdade desde sempre, sem eles nada disso seria realidade. Agradeço também aos meus amigos que fiz durantes todos esses anos e também a todos os professores que contribuíram para minha formação.

7. REFERÊNCIAS

[1] 5 things to know about Americans and their smart speakers. Pew Research Center, Washington DC, 21 Nov de 2019, Disponível em: https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/ Acesso em: 13/10/2022.

[2] Mobile Fact Sheet. Pew Research Center, Washington DC, 07 Abr de 2021, Disponível em: https://www.pewresearch.org/internet/fact-sheet/mobile/. Acesso em : 14/10/2022.

[3] Silva, Diana, Mariana Curado Malta, Paulo Alves de Sousa de Vasconcelos. "Desafios da Privacidade nos Assistentes Virtuais Pessoais." *Cadernos de Investigação do Mestrado em Negócio Eletrónico* 2 (2022). Disponível em: https://www.iscap.pt/ebusiness-rj/index.php/mne-rj/article/view/194/181. Acesso em: 20/10/2022.

[4] Amazon Workers Are Listening to What You Tell Alexa. Bloomberg, Ago 3 de 2019, Disponível em: https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio Acesso em: 08/11/2022.

[5] Yep, human workers are listening to recordings from Google Assistant, too. The Verge, 11 Jul de 2019, Disponível em: https://www.theverge.com/2019/7/11/20690020/google-assistant-home-human-contractors-listening-recordings-vrt-nws Acesso em: 08/11/2022.

[6] Bolton, T., Dargahi, T., Belguith, S., Al-Rakhami, M. S., & Sodhro, A. H. (2021). On the security and privacy challenges of virtual assistants. Sensors, 21(7), 2312. https://doi.org/10.3390/s21072312

[7] Rawassizadeh, R., Sen, T., Kim, S. J., Meurisch, C., Keshavarz, H., Mühlhäuser, M., & Pazzani, M. (2019). Manifestation of virtual assistants and robots into daily life: Vision and challenges. CCF Transactions on Pervasive Computing and Interaction, 1(3), 163-174. https://link.springer.com/article/10.1007/s42486-019-00014-1

[8] Cheng, P. & Roedig, U. Personal Voice Assistants Security and Privacy—A Survey. Disponível em: https://ieeexplore.ieee.org/document/9733178 Acesso em: 15/11/2022

[9] Yan, C & Ji, X & Wang, K & Jiang, Q & Jin, Z & Xu, W. A Survey on Voice Assistant Security: Attacks and Countermeasures. Disponível em: https://dl.acm.org/doi/10.1145/3527153 Acesso em: 15/11/2022.

[10] Cunneen, M., Mullins, M., & Murphy, F. (2020). Artificial intelligence assistants and risk: framing a connectivity risk narrative. Ai & Society, 35(3), 625-634. https://link.springer.com/article/10.1007/s00146-019-00916-9

[11] New York Times [Internet]. 2019. Ago 21. Disponível em: https://www.nytimes.com/2019/08/21/technology/personaltech/alexa-siri-google-assistant-listen.html). Acesso em: 10/12/2022.

[12] Paula, Marcus Vinícius Cândido de. Segurança da informação e a internet das coisas. Monografia (Graduação em Engenharia da Computação) - Faculdade de Tecnologia e Ciências Sociais Aplicadas. Centro Universitário de Brasília. 2020. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/15108/1/Projeto_Final_EC_Marcus_RA_21706888_POS_BANCA_FINAL.pdf. Acesso em: 03/01/2023.