Contemporânea
Contemporary Journal
Vol.x No.x: 01-xx, 2024
ISSN: 2447-0961

Artigo

RISCOS DE SEGURANÇA EM ASSISTENTES VIRTUAIS

SECURITY RISKS IN VIRTUAL ASSISTANTS

RIESGOS DE SEGURIDAD EN ASISTENTES VIRTUALES

DOI: 10.56083/RCVXNX-
Receipt of originals: 18/11/2024
Acceptance for publication: XX/XX/2024

Danilo Mendonça Barbosa
Engenharia da computação - tecnologia
Instituição de formação: Universidade São Judas Tadeu
Endereço: São Paulo, SP - Brasil
E-mail: danilomb99@gmail.com

Henrique Menezes
Engenharia da computação - tecnologia
Instituição de formação: Universidade São Judas Tadeu
Endereço: São Paulo, SP - Brasil
E-mail: henriquemenezes0@gmail.com

Pedro Henrique Custódio Ignácio
Engenharia da computação - tecnologia
Instituição de formação: Universidade São Judas Tadeu
Endereço: São Paulo, SP - Brasil
E-mail: pedrohcijgm01@gmail.com

Pedro Henrique de Oliveira Caló
Engenharia da computação - tecnologia
Instituição de formação: Universidade São Judas Tadeu
Endereço: São Paulo, SP - Brasil
E-mail: pedrohocalo@gmail.com

Prof. Msc. Roberto Marcos Kalili
Mestre em Administração Financeira
Instituição de formação: UPM
Endereço: São Paulo, SP - Brasil
E-mail: prof.kalili@usjt.br

RESUMO: Ao decorrer desse artigo buscou-se entender os principais pontos acerca dos riscos à privacidade causados por assistentes virtuais, tais como a Alexa ou o próprio assistente do Google. Em um primeiro momento, se fez necessário entender a forma como a maior parte das pessoas enxergam tais assistentes e os riscos trazidos pelos mesmos. A partir da obtenção dessa compreensão popular, o artigo se propõem a expor quais são os riscos que um assistente virtual pode ter na privacidade de cada um, seja por meio de ataques de terceiros com intenções contrárias, ou até mesmo na permissibilidade que se consegue a tais assistentes quando se aceita os termos de utilização. Mediante a tal, o artigo também elenca os principais tópicos de políticas de privacidade desses assistentes, trazendo quais os dados capturados e como funciona a tratativa dessas informações pelas empresas proprietárias dos assistentes virtuais, escorando sempre na LGPD (Lei Geral de Proteção de Dados). Por fim, o artigo tem como objetivo trazer formas mais eficazes para se resguardar e prevenir que dados sensíveis sejam vazados ou utilizados para fins das quais o usuário, muitas das vezes, não está totalmente ciente.

PALAVRAS CHAVE: Assistentes-Virtuais, privacidade, LGPD, Segurança.

ABSTRACT: This article explores the privacy risks posed by virtual assistants such as Alexa and Google Assistant. It begins by examining how most people perceive these devices and the associated risks. Based on this understanding, the article identifies the specific privacy threats, including vulnerabilities to external attacks and the permissions granted to these assistants when users accept terms of service. Additionally, it outlines key points from the privacy policies of these assistants, detailing the types of data collected and how this information is handled by the companies, in compliance with the General Data Protection Law (LGPD). Finally, the article aims to provide effective strategies for users to safeguard their sensitive data and prevent leaks or misuse that they may not fully understand.

KEYWORDS: Virtual assistants, Privacy, LGDP, Security.

RESUMEN: A lo largo de este artículo se buscó comprender los principales puntos relacionados con los riesgos a la privacidad causados por los asistentes virtuales, tales como Alexa o el propio asistente de Google. En un primer momento, fue necesario entender cómo la mayoría de las personas perciben dichos asistentes y los riesgos que conllevan. A partir de esta comprensión popular, el artículo se propone exponer cuáles son los riesgos que un asistente virtual puede representar para la privacidad de cada individuo, ya sea a través de ataques de terceros con intenciones maliciosas o incluso debido a la permisividad otorgada a estos asistentes al aceptar los términos de uso. En este contexto, el artículo también enumera

los principales puntos de las políticas de privacidad de estos asistentes, destacando qué datos se recopilan y cómo las empresas propietarias de los asistentes virtuales tratan dicha información, apoyándose siempre en la LGPD (Ley General de Protección de Datos). Por último, el objetivo del artículo es presentar formas más eficaces de protegerse y prevenir que datos sensibles sean filtrados o utilizados para fines de los cuales, en muchas ocasiones, el usuario no está completamente consciente.

PALABRAS CLAVE: Asistentes virtuales, Privacidad, LGDP, Seguridad.

1. Introdução

Com a crescente evolução tecnológica nos últimos anos, assistentes virtuais têm se tornado cada vez mais presentes em ambientes domésticos. De diversas formas, seja em aparelhos próprios para essas tarefas como a Alexa da Amazon, ou até mesmo nos próprios celulares, como é o caso de assistentes como Google Assistant e Siri da Apple. Tais dispositivos possuem a função de auxiliar seus usuários, automatizando controles domésticos por comando de voz, marcando compromissos na agenda, enviando mensagens para contatos, entre outras funções. Em contrapartida, assistentes virtuais coletam diversos dados sensíveis de monitoramento, rotina e padrões do usuário, os quais podem causar prejuízos caso sejam vazados para terceiros que os utilizem para benefício próprio. Dados de rotina podem servir tanto para direcionar conteúdos e propagandas ao usuário, como também serem usados por pessoas para cometer fraudes e aplicar golpes. Portanto, se faz necessário (i) entender os principais riscos que conceder informações à assistentes virtuais pode gerar, por meio do entendimento das diretrizes de uso e percepções populares. Adiante, (ii) encontrar a forma mais eficaz para evitar possíveis vazamentos de dados sensíveis e prejuízos ao usuário, analisando tecnologias do mercado e se ancorando na LGPD (Lei Geral de Proteção de Dados).

2. Assistentes Virtuais

Assistentes virtuais, como popularmente conhecidos, são dispositivos eletrônicos que auxiliam na realização de tarefas. Com a rápida evolução tecnológica nos últimos anos, e também com um desejo cada vez maior da individualização de dispositivos eletrônicos, os assistentes virtuais se tornaram cada vez mais comuns em ambientes domésticos. Alguns dos mais famosos são: A Alexa da Amazon, o Google Assistant que vem acompanhado em smartphones com o sistema operacional Android, a Bixby da Samsung, Siri da Apple, entre outros.

Segundo uma pesquisa da Forbes em 2022, mais de 5 bilhões de pessoas já estavam ativamente conectadas à internet. As tarefas que cada pessoa realiza são as mais diversas, redes sociais, canais de entretenimento, portais de notícia, armazenamento de dados, e até mesmo para uso profissional. Em outras palavras, um grande número de pessoas online, junto de uma possibilidade infinita de atividades, faz com que gere uma necessidade de tecnologias e dispositivos que auxiliem essa navegação, levando o usuário diretamente pro ponto onde quer estar.

Nas palavras de Antônio Juarez Alencar, Eber Assis Schmitz e Leôncio Teixeira Cruz (Assistentes Virtuais Inteligentes: Conceitos e estratégias, 2013) "Em síntese, os assistentes virtuais inteligentes propiciam a nossos clientes experiências prazerosas e enriquecedoras ao utilizarem os produtos e serviços que oferecemos". Facilitam e otimizam buscas, ações e tempo, tornando-se assim, cada vez mais indispensáveis no cotidiano popular.

A Alexa tem se tornado um dos assistentes virtuais com maior popularidade para o público geral no mercado. Apresentada para o mundo em 2014 pela Amazon, a assistente consta com diversas funções de otimização, que se conecta com casas inteligentes, responde dúvidas, envia mensagens, realiza ligações, até mesmo conta piadas, entre outras

funções. Em uma pesquisa realizada por formulário popular, foi apontado que a Alexa é a segunda assistente mais utilizada, perdendo apenas para o google assistant, que já vem instalado em celulares com o sistema operacional Android.

Uma das empresas com maior influência no mercado digital também possui seu próprio assistente virtual, o Google Assistant, lançado em meados de 2016 pela Google. Em comparação com a Alexa, por exemplo, as duas tecnologias são bastante similares, porém o que diferencia o assistente da Google é o fato de vir instalado em dispositivos Android. Tal fato faz com que seja o assistente virtual de maior utilização no mercado, muitas pessoas talvez nem se dêem conta que o estão utilizando, já que pode facilmente ser confundido com o próprio pesquisador do Google.

3. Políticas de Privacidade de Assistentes Virtuais

Um ponto importante a se considerar quando se fala na privacidade e segurança de dados em assistentes virtuais é sua própria política de dados disponibilizada pela empresa ou fabricante. Pois em tese, tais dispositivos não podem coletar informações a mais não especificadas nessas diretrizes, porém essas políticas de dados também podem pender para o outro lado. Em uma pesquisa popular realizada para o melhor entendimento do assunto, mais de 80% das pessoas que responderam afirmaram não terem lido as diretrizes e políticas de privacidade de assistentes virtuais.

Segundo Lima (2014), empresas que fornecem serviços online tendem a disponibilizar os termos de contrato de privacidade de maneira muito técnica e longa. O usuário, muitas vezes motivado pelo desejo de um consumo imediato e se utilizando de "boa fé", junto da dificuldade de compreensão dos longos contratos, concorda sem ao menos ler.

Como dito por Bolton (2021), gravações podem ser armazenadas sem o consentimento do usuário por estarem sempre conectadas à internet.

Porém, segundo a Amazon, essas gravações somente são concluídas se o dispositivo confirmar a palavra de ativação, que nesse caso seria “Alexa”. A Amazon também disponibiliza nas configurações do dispositivo a opção de excluir as solicitações gravadas.

Existe também a opção de que a ativação seja realizada através de um botão, evitando que palavras similares à palavra de ativação permitam gravações que não deveriam ser feitas. Para o caso do Echodot, existe um botão que desliga o microfone, e com essa função desabilitada o dispositivo não conseguirá fazer a captura de nenhum áudio. Em 2019, uma reportagem feita pela CBS revelou que, naquele ano, a Amazon continha um certo número de funcionários que ouviam algumas gravações de clientes ao longo do dia, esses funcionários então transcreviam essas informações e incluíam no serviço de treinamento da IA utilizado para o reconhecimento de voz e NLP.

NLP, Natural Language Processing ou Processamento de linguagem natural pode ser definido como a capacidade de um algoritmo em traduzir entradas (seja texto, voz ou outras fontes) em uma linguagem que a máquina possa entender e direcionar a tarefa da qual precisa realizar. Como concluem Nesi, Pantaleo e Sanesi (2015), NLP é a tecnologia que permite que um dispositivo absorva uma informação legível através de dados de linguagem natural não estruturados. Na óptica de assistentes virtuais essa tecnologia é de extrema importância, e precisa ser cada vez mais treinada, já que usuários muitas vezes falam ou escrevem que desejam para seus assistentes da mesma forma da qual conversam com um amigo.

Porém a Amazon também afirmou ter profissionais de segurança que vigiam tal serviço e possuem uma tolerância zero para qualquer tipo de uso indevido com os dados dos clientes, sem contar no fato de que os funcionários não conseguiam saber quem eram os clientes das quais eles

estavam ouvindo a gravação, impedindo assim que alguém utilizasse essa informação em benefício próprio.

Existem também aparelhos ou aplicativos terceiros conectados a assistentes virtuais também podem receber informações do usuário que são captadas pelos dispositivos. Caso um aplicativo necessite da sua localização, e ele esteja integrado à sua Alexa, a localização será enviada para esse aplicativo e estará sujeita não mais às políticas de privacidade do assistente virtual, mas sim do aplicativo.

Cookie e dados de navegação também são armazenados em assistentes virtuais, esses dados são utilizados para promover uma publicidade personalizada, por isso é comum que ao pesquisar sobre um produto, ou entrar em algum site específico, propagandas relacionadas àquele produto ou ao gênero do site se tornem mais comum em seus feeds.

Um ponto importante a salientar é o fato de que o usuário muitas vezes é induzido a aceitar os termos de uso para fazer o proveito de uma tecnologia. Segundo os próprios termos da Alexa (Atualizados em 20 de setembro de 2023): "Se você não aceitar os referidos termos, não poderá usar a Alexa." Em outras palavras, o usuário sabe que precisa realizar aquele aceite para a utilização de um assistente virtual. Tanto esse termo específico quanto também o fato de que, muitas vezes, os mesmos são escritos de uma maneira muito rebuscada, e pouco popular, dificultando a total compreensão do usuário, fazem com que o usuário simplesmente se submeta a entregar e aceitar qualquer coleta de dados imposta pela empresa do assistente virtual.

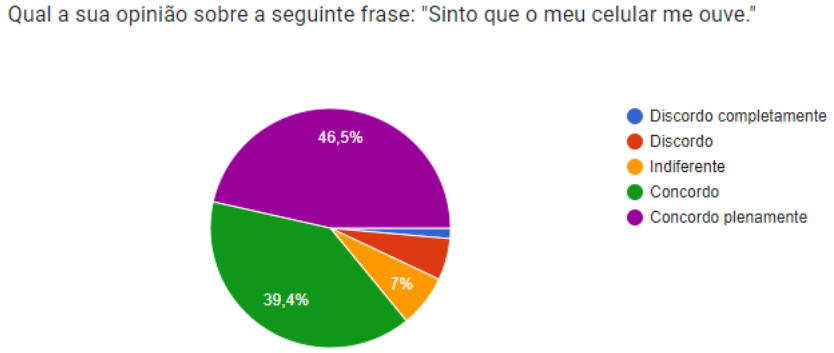
Ademais, existe uma quantidade massiva de informações sensíveis armazenadas em nuvens e servidores de empresas prestadoras de serviços online ou de assistentes virtuais, que se não forem eficazmente resguardadas e protegidas, podem se tornar alvos fáceis para hackers e

golpistas que se utilizam desses dados para fins próprios que levarão danos ao usuário.

4. Riscos à Segurança e Privacidade do Usuário

Para escolher e elencar os métodos mais eficazes a fim de proteger a segurança e privacidade dos usuários de assistentes virtuais, é necessário, primeiramente, descrever e compreender os riscos existentes no uso de tais tecnologias. Esses riscos são numerosos e podem impactar diretamente na percepção dos usuários sobre a segurança dos dispositivos. Dentre os principais problemas relatados, um dos mais alarmantes é a frequente e ininterrupta gravação de áudio, de acordo com pesquisa realizada:

Imagem 2: preocupação dos usuários quanto à gravação constante de áudio



Fonte: pesquisa realizada com voluntários, 2024.

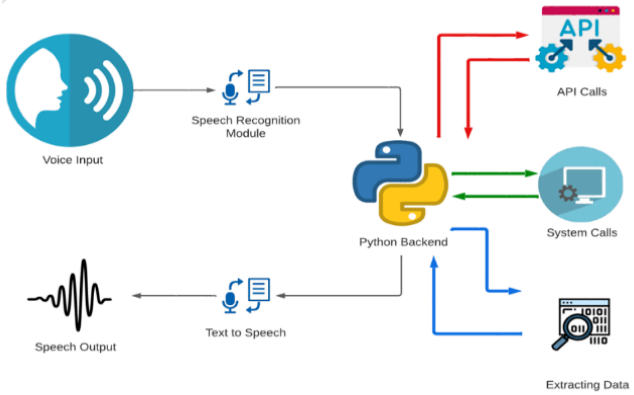
Segundo matéria publicada em 2021 no site Agemt da PUCSP (Pontifícia Universidade Católica de São Paulo):

> Do ponto de vista técnico, os assistentes virtuais são um conjunto de microfones, ligados a um alto-falante, que são controlados por um processador que pode enviar e receber informações da nuvem, onde esses dados são processados. Com a ajuda de algoritmos de inteligência artificial, implementados na nuvem e sempre atualizados no processador, o aparelho traz respostas rápidas.

Mesmo que estes dispositivos respondam apenas após receberem comandos específicos, seus microfones permanecem sempre ativos a fim

de detectar tais comandos, fazendo com que, na prática, conversas privadas sejam capturadas e enviadas para os servidores das empresas responsáveis, sem autorização explícita ou consciente por parte dos usuários, conforme visto na imagem abaixo:

Figura 3: exemplo de fluxo dos comandos de voz de um assistente virtual



Fonte: IJRASET (International Journal for Research in Applied Science and Engineering Technology), 2022.

Tal comportamento gera a sensação de invasão constante, uma vez que, mesmo em situações domésticas, há a possibilidade da gravação de informações sensíveis sem aviso prévio, o que já aconteceu. Segundo matéria publicada no site El País (2019), a empresa de tecnologia Google, respondendo a uma reportagem do canal belga de notícias VRT NWS, admitiu que 0,2% dos áudios gravados por seus dispositivos passam por análises humanas, o que compromete a privacidade dos usuários. Apesar da gigante da tecnologia esclarecer que esses áudios foram enviados à "especialistas da linguagem" de vários países apenas para uma rápida transcrição e entendimento de frases não conectadas aos usuários, o canal belga obteve acesso a cerca de mil áudios anônimos e foi capaz de "identificar endereços postais e outras informações sensíveis", conseguindo até mesmo encontrar um casal de Waasmunster (Bélgica), o qual "reconheceu imediatamente a voz de seu filho e do seu neto". Embora o Google tenha dito que os assistentes enviam os áudios apenas quando identificam alguma palavra chave ('Ok Google', por exemplo), segundo o El

País, “a VRT NWS disse que, de cerca de mil falas à quais teve acesso (todas em holandês), 153 eram conversas em que o assistente foi acionado sem ninguém ordenar”.

Tendo em vista este caso, a preocupação com a coleta e tratativa de dados se torna mais justificada, porém, áudios gravados não são a única informação preocupante. Outro ponto que merece atenção é a captura de imagens por dispositivos equipados com câmeras, sejam elas embutidas no assistente ou conectadas por meio de dispositivos complementares, como babás eletrônicas e câmeras de vigilância.

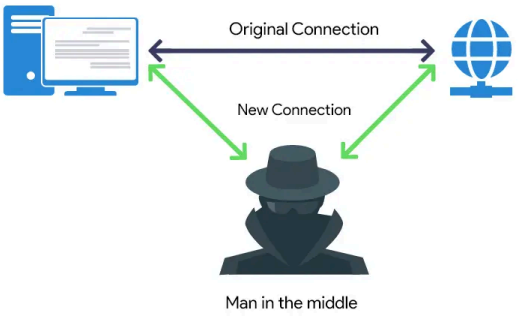
Embora essas tecnologias sejam vendidas como formas convenientes de monitoramento remoto, como pais acompanhando seus bebês à distância ou sistemas de vigilância caseira, também abrem margem para o risco de invasão de privacidade. Imagens e vídeos gravados em tempo real podem ser interceptados e utilizados por indivíduos maliciosos, expondo pessoas e ambientes sem o conhecimento do usuário. A preocupação aumenta se considerarmos que os dispositivos, quando armazenam e transmitem dados visuais, podem se tornar alvos de invasores interessados em mapear padrões de comportamento ou monitorar atividades cotidianas.

Em matéria publicada no site O Globo (2023), a Comissão Federal do Comércio (FTC, na sigla em inglês), realizou uma denúncia à Amazon, que foi acusada pela espionagem de mais de 80 mulheres por meio de um dispositivo denominado ‘Ring Stick Up Cam’, o qual fora lançado em 2014 com o intuito de permitir o monitoramento de ambientes online por seus usuários. Entretanto, em 2017, um funcionário da Ring, empresa adquirida posteriormente pela Amazon e responsável pela produção das câmeras, obteve acesso a inúmeras gravações de no mínimo 81 mulheres por meio do dispositivo. A gigante da tecnologia concordou em pagar quase 6 milhões de dólares pelo ocorrido.

Além dos riscos relacionados à coleta e transmissão de dados sensíveis, há também o risco na realização de compras por meio de comandos de voz. Alguns assistentes virtuais, como a Alexa da Amazon ou Bixby da Samsung, possuem a configuração de operar vinculados à contas pessoais, permitindo, assim, que o usuário faça compras apenas com comandos de voz, sem precisar de senhas ou outras etapas de autenticação. Ainda que essa funcionalidade seja conveniente, ela traz a possibilidade de abusos, como compras não autorizadas por crianças ou mesmo por terceiros com acesso ao dispositivo, por exemplo. Em casos mais extremos, a realização de compras indevidas pode resultar em prejuízos financeiros para o usuário da conta, principalmente se medidas adicionais de controle não forem utilizadas, como confirmações de segurança ou restrições de voz.

Além dos riscos funcionais, há pesquisas que têm validado preocupações sobre a vulnerabilidade dos assistentes virtuais. Segundo o site Tecmundo (2020), em um estudo realizado com o dispositivo Alexa, da Amazon, pesquisadores da empresa de tecnologia Check Point Security descobriram falhas no tráfego de informações entre o assistente e os servidores. Na pesquisa, foi demonstrado que, ao interceptar a comunicação utilizando um ataque conhecido como Man-in-the-middle, é possível acessar dados sensíveis, tanto do dispositivo quanto do usuário, o que abre caminho para possíveis ações maliciosas. Dentre as possibilidades mais graves, identificaram a instalação silenciosa de skills (aplicativos) com o objetivo de monitorar comportamento dos usuários, capturar suas credenciais e até mesmo controlar dispositivos remotamente, como câmeras e dispositivos de segurança conectados ao assistente, sem o conhecimento da vítima.

Figura 4: Ataque Man-in-the-middle, utilizado para interceptar dados do usuário



Fonte: Beagle Security

Outra pesquisa revelou um método inovador, porém preocupante, de exploração. De acordo com pesquisadores da universidade de Zhejiang, na China, o método denominado "dolphin attack" (ataque de golfinho, em tradução livre), faz uso de frequências ultrassônicas – inaudíveis aos ouvidos humanos, mas detectadas por microfones – para o envio de comandos ocultos. Através desta técnica, é possível disfarçar um comando, como 'Ok Google, abrir o portão da frente' ou 'Hey siri, ativar modo avião', em uma música ou áudio aparentemente inofensivo. Nesta situação, uma vulnerabilidade significativa é criada, principalmente em ambientes altamente conectados, com um grande número destes dispositivos, onde uma simples execução automática pode pôr em risco a segurança física e patrimonial dos usuários. O uso de tecnologias sofisticadas como essa demonstra como o uso cada vez mais frequente de assistentes virtuais exige máxima atenção para a detecção e mitigação de novas ameaças.

5. LGPD e IA

Quando se fala em LGPD (Lei Geral de Proteção de Dados, L13709) e IA, são grandes forças que mudaram muito no nosso século, pois estabelece grande marco regulatório para o tratamento das informações, já a IA oferece um potencializador na inovação e otimização dos procedimentos, sendo até para apoiar a legislação na leitura destes

processos como descrito por ABRAMOWICZ et al (2024) mencionando esse potencial para analisar dados e identificar cláusulas que não tem conformidade com a legislação.

É de conhecimento popular que esse assunto é desafiador pois em muitas empresas e negócios esse sistema de IA foi embutido, resultando em vários desafios de LGPD. A IA por si coleta, armazena e analisa um volume imenso de dados gerados, sejam eles sensíveis ou não, lembrando que isso é essencial para sua funcionalidade como uma assistente virtual, Aline Noleto et al (2023) em seu artigo diz que um assistente virtual utiliza dessas informações para poder entregar um serviço mais personalizado e otimizado com as preferências de seu usuário. Aline Noleto também nos diz que tudo isso deve ser feito em conformidade com os princípios de LGPD, tais princípios abordam a fidelidade dos dados que devem ter função legítima, adequação específica devendo ser relevantes e limitados, transparência pois os honorários de suas informações devem ser relatados sobre o tratamento do mesmo e o principal é a segurança para a proteção contra acessos não autorizados ou tratamento dos dados de formas ilícitas.

Logo, um assistente virtual que esteja em linha com a LGPD teoricamente é seguro, pois a utilização de dados pessoais serão limitados e com funções atribuídas descritas por Jerusa (2024) que para o uso correto controlador deve ser exigente e se atentar às leis da LGPD na hora da implementação com as assistentes virtuais. Com o uso inadequado da ia pode trazer malefícios a empresa, como vazamentos de dados sensíveis, lembrando que toda IA seja implementada em uma empresa ou não, tem como o enriquecimento de dados conforme o cliente utiliza para pesquisa ou enviando novos dados para tratamento, ou mais a fundo cada colaborador de uma empresa usa.

A maior preocupação das empresas quando utilizam uma IA para qualquer tipo de integração com seu sistema é a segurança dos seus

dados, e sim, nunca se pode garantir 100% de segurança. Recentemente noticiado pelo blog de segurança Security Report (2024) ocorreu um caso de grande relevância, houve um vazamento de dados com a ferramenta Chat GPT, várias contas de acessos foram expostas na Deep Web, assim colocando em risco as pessoas e suas informações como senhas e endereços, a desenvolvedora negou as acusações dizendo que isso aconteceu devido às softwares infectados com malwares nos dispositivos dos usuários, isso foi um grande incidente em 2023 alertando os riscos a ferramentas de IA.

Existe um regulamento que está sendo implantado porém já em vigor pelo Poder Executivo, o chamado Projeto de Lei n° 2338 escrito por Rodrigo Pacheco Senador (2023), entretanto ainda não tem uma aprovação geral, ou seja, muitos usam a ética das empresas fornecedoras de IA e também as leis para que assim consigam tratar informações sensíveis de forma restrita.

5.1 Fundamentos da LGPD

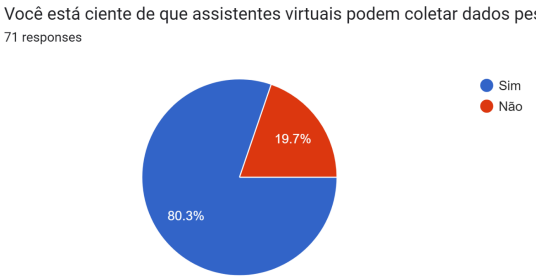
A LGPD visa regulamentar o processo da tratativa de dados sensíveis por meio de empresas prestadoras de serviço, para que se possa defender o usuário final de possíveis vazamentos de dados e informações pessoais que possam trazer prejuízo ao usuário. Assim como defendido por Maria Eugenia Finkelstein e Claudio Finkelstein (2019), a LGPD se faz necessária para a criação de um ambiente social saudável, seja ele online ou não. Já que com a constante evolução tecnológica, cada vez mais esse dinamismo se aproxima do usuário final, seja com propagandas de lojas, anúncios de eventos, recomendações de conteúdos online, ambos voltados para o gosto do usuário, baseado em suas informações e dados de navegação. Em outras palavras, dados pessoais têm se tornado uma importante moeda de troca, de alto valor, para grandes corporações, já que coletam dados do

usuário e os utilizam para saber o que oferecer ao mesmo em seguida. Porém também é necessário que nesse cenário haja leis e normas que defendem o usuário final do uso exacerbado, ou não tratado corretamente, de seus dados pessoais. Para que tenha um respaldo de navegar na internet, e utilizar dispositivos como assistentes virtuais, sem que lhe cause um prejuízo futuro.

6. Formas De Proteção De Segurança E Privacidade Do Usuário

Segundo o jornal O Globo, em uma pesquisa realizada em 2023, 67% dos brasileiros utilizam assistentes virtuais, e com a crescente popularidade surgem dúvidas com base na privacidade. É de comum conhecimento que esses assistentes utilizam comandos de voz para serem ativados, e isso leva os dispositivos a estarem constantemente procurando por esses comandos, o que faz com que os mesmos utilizem o microfone do aparelho, quase que 100% do tempo.

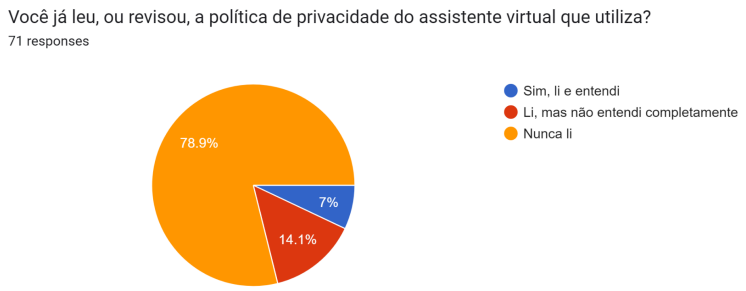
Figura 5: Consciência de coleta de dados feita durante o uso de assistentes



Fonte: pesquisa realizada com voluntários, 2024.

A pesquisa feita para o artigo aponta que cerca de 20% das pessoas que responderam não têm o conhecimento que os assistentes virtuais podem estar coletando dados pessoais do usuário. E ainda se afirma que 92% das pessoas não leram os termos de uso dos assistentes utilizados; e desse grupo contemplado 14% leu e não entendeu plenamente esses termos de uso.

Figura 6: leitores dos termos de de política de privacidade



Fonte: pesquisa realizada com voluntários, 2024.

Devido à falta de conhecimento das pessoas em relação aos limites dos assistentes virtuais, se dá por requisito conhecer algumas maneiras de proteger dados sensíveis dos usuários.

Quando se observa o uso frequente dos assistentes é recomendado, pelo suporte da empresa Google, que o usuário bloqueie o acesso ao assistente de aplicativos terceiros. Os próprios assistentes oferecem uma grande segurança para o usuário, mas quando o usuário permite o acesso de aplicativos terceiros se cria uma outra forma de "invadir"e roubar os dados privados armazenados nos bancos de dados dos assistentes. E quanto a esses dados armazenados recomenda-se a limpeza frequente, onde, em caso de invasão, permite com que os invasores se deparem com um banco de dados sem nenhuma informação que possa ser utilizada para fraudes ou roubos.

Os assistentes mais comuns utilizam de uma membrana, chamada diafragma, que capta as vibrações do ar e transforma em sinais elétricos para que possam ser interpretados pelo sistema. A pesquisadora da Universidade de Michigan, e coautora da pesquisa, Sara Rampazzi descobriu uma falha no sistema, que consiste em mudar a intensidade da luz modulando os comandos de voz. A pesquisa mostra que a primeira geração do Echo Plus e do Google Home podem sofrer de ataques com distâncias superiores a 110 metros, e isso acontece por uma falha no próprio design dos aparelhos, que foram desenvolvidos com sensores mais

sensíveis, para serem utilizados em ambientes domésticos e acessados a uma certa distância. Segundo a pesquisadora, "Você precisa comprar um equipamento para alterar a corrente elétrica do laser e ter informações sobre como funciona a modulação. Definitivamente, não é algo simples, mas nós mostramos que é possível".

Infelizmente não existe nenhum método que seja 100% eficaz quando falamos de segurança online. A tecnologia está cada vez mais avançada e instiga a aparição de novos problemas, fazendo com que os métodos de segurança online precisem sempre estar atualizados para garantir a proteção dos dados dos usuários. Nenhum dos métodos citados acima vão garantir uma proteção completa, porém, quanto menor o número de vulnerabilidades, maior a garantia que os seus dados não serão roubados. Quanto maior o número de obstáculos que os invasores precisarem passar para ter acesso à conta, menor a chance desse ataque ser bem sucedido e causar prejuízo.

7 Conclusão

Atualmente é possível enxergar um crescente aparecimento de assistentes virtuais em ambientes domésticos e no cotidiano das pessoas. Eles ajudam a se obter uma navegação mais rápida e fácil, cortando caminhos, personalizando a experiência do usuário e até mesmo contando piadas quando solicitado. Porém, a massiva quantidade de dados de rotina e informações sensíveis que são utilizadas e armazenadas por esses assistentes virtuais podem vir a se tornarem um problema vindouro para seu usuário. Como abordado pelo artigo, e demonstrado através de pesquisas populares, grande parte dos usuários não leem os contratos de uso e nem sequer sabem quais dados pessoais e sensíveis estão sendo utilizados pelo assistente virtual, e para qual função. É fato que a falta de transparência e clareza das empresas fabricantes desses assistentes é um

ponto forte para gerar essa ignorância. Porém, a falta de conhecimento do usuário, junto com falhas de segurança, fazem com que existam diversas formas e brechas que podem ser utilizadas por pessoas com más intenções para se obter vantagem. Desde vazamentos de áudio e câmeras de segurança, até mesmo ataques externos que podem fazer com que seu assistente virtual abra a porta da sua casa. Ou seja, ao mesmo tempo que facilitam a vida do usuário quanto a navegação, podem acabar trazendo prejuízo caso não seja dada a devida atenção e proteção. Criação de senhas fortes, adição de verificações de etapas adicionais para tarefas críticas e gerenciamento das conexões entre dispositivos terceiros são algumas das formas que o usuário encontra para se prevenir. A verdade é que não existe uma forma de se proteger 100%, é um risco do qual se assume, mas mitigar e prevenir esses riscos é possível, e normalmente funcional. Nas palavras de Isaac Asimov "Se o conhecimento pode criar problemas, não é através da ignorância que podemos solucioná-los", conhecer os dispositivos e normas dos assistentes dos quais confiam seus dados pessoais, é de extrema importância para que cada vez mais se possa ter uma navegação otimizada, individualizada, mas sobretudo segura.

Referências

MICHAEL, Melissa. **Attack Landscape H1 2019:** IoT. F-Secure, 2019. Disponível em: https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

BARDA, Dikla; ZAIKIN, Roman; SHRIKI, Yaara. **Keeping the gate locked on your IoT devices:** Vulnerabilities found on Amazon's Alexa. Check Point Research, 2020. Disponível em: https://research.checkpoint.com/2020/amazons-alexa-hacked/.

KUKSOV, Igor. **Assistentes de voz ouvem coisas que nós não ouvimos.** Kaspersky, 2019. Disponível em: https://www.kaspersky.com.br/blog/ultrasound-attacks/11409/

SIDELL, Elle Poole. **A Alexa está sempre ouvindo? Como proteger a sua privacidade?**. Avast, 2021. Disponível em: https://www.avast.com/pt-br/c-amazon-alexa-listening

MACHADO, Charles. **Assistentes Virtuais e a Sua Privacidade, Quais os Riscos?**. Jusbrasil, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/assistentes-virtuais-e-a-sua-privacidade-quais-os-riscos/1301081492

CROSS, R. J. **Is Alexa always listening? How to protect your data from Amazon**. U.S. Pirg, 2024. Disponível em: https://pirg.org/edfund/resources/alexa-listening-explainer/

BRADFORD, Alina. **Can Alexa Be Hacked? Here's How To Prevent It**. Family handyman, 2024. Disponível em: https://www.familyhandyman.com/article/can-alexa-be-hacked/

LINSKEY, Dorian. **'Alexa, are you invading my privacy?'** – the dark side of our voice assistants. The Guardian, 2019. Disponível em: https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants

HUB, Blockchain. **Smart Home Devices and Privacy Risks:** Is Your Alexa Spying on You?. Medium, 2023. Disponível em: https://medium.com/@abrahamedet9/smart-home-devices-and-privacy-risks-is-your-alexa-spying-on-you-e9f4e0465a4d

PICCHI, Aimee. **Amazon workers are listening to what you tell Alexa**. CBS News, 2019. Disponível em: https://www.cbsnews.com/news/amazon-workers-are-listening-to-what-you-tell-alexa/

ABRAMOWICZ, João Freire; SILVA, Heuryk Wylk Ébolida. **Uso da inteligência artificial (IA) na análise de identificação à Lei Geral de Proteção de Dados (LGPD)**. HUMANAE Questões controversas do mundo contemporâneo,v.18, n.2, 2024. Disponível em: https://revistas.esuda.edu.br/index.php/humanae/article/view/982/435

NOLETO, Aline; DOMINGUES, Patrícia. **Marco Legal da IA e LGPD:** Novos Desafios na privacidade e enriquecimento de Dados. Consultor Juridico, 2023. Disponível em: https://www.conjur.com.br/2023-dez-06/marco-legal-da-ia-e-lgpd-novos-desafios-na-privacidade-e-enriquecimento-de-dados

BOHRER, Jerusa. **Inteligência Artificial e Proteção de Dados**. Implementado a LGPD, 2024. Disponível em: https://www.implementandoalgpd.com.br/blog/inteligencia-artificial-e-protecao-de-dados

ZENDESK. **IA na segurança e privacidade de dados:** usos, impactos e riscos. Blog da Zendesk, 2024. Disponível em: https://www.zendesk.com.br/blog/ia-na-seguranca-e-privacidade-de-dados

REDAÇÃO. **Vazamento do ChatGPT afeta mais de 6.500 brasileiros e 100 mil no mundo**. Security Report, 2023. Disponível em: https://securityleaders.com.br/vazamento-do-chatgpt-afeta-mais-de-6-500-brasileiros-e-100-mil-no-mundo

BOLTON, Tom; DARGAHI, Tooska; BELGUITH, Sana; AL-RAKHAMI, Mabrook S.; SODHRO, Ali Hassan. **On the security and privacy challenges of virtual assistants**. Multidisciplinary Digital Publishing Institute, 2021. Disponível em: https://www.mdpi.com/1424-8220/21/7/2312

FERNANDES, Luiza. **Uso de assistentes digitais causa controvérsia por uso de dados pessoais**. Agência de Jornalismo online da PUC-SP, 2021. Disponível em: https://agemt.pucsp.br/noticias/uso-de-assistentes-digitais-causa-controversia-por-uso-de-dados-pessoais

GUPTA, Ujjwal; JINDAL, Utkarsh; GOEL, Apurv; MALIK, Vaishali. **Desktop Voice Assistant**. International Journal for Research in Applied Science and Engineering Technology, 2022. Disponível em: https://www.ijraset.com/research-paper/desktop-voice-assistant

PROTECT your personal information and data. Federal Trade Commission Consumer Advice, 2021. Disponível em: https://consumer.ftc.gov/articles/protect-your-personal-information-and-data

PROTECT my privacy online. University of Oxford, 2018. Disponível em: https://www.infosec.ox.ac.uk/protect-my-privacy-online

POPHAM, John. **Largest study of its kind shows outdated password practices are widespread**. Georgia Tech, 2023. Disponível em:https://www.cc.gatech.edu/news/largest-study-its-kind-shows-outdated-password-practices-are-widespread

WAMSLEY, Laurel. **Your technology is tracking you**. National Public Radio, 2020. Disponível em: https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy

STEELE, Marcus. **Maintaining your online privacy**. National Institute of Standards and Technology, 2021. Disponível em: https://www.nist.gov/blogs/manufacturing-innovation-blog/maintaining-your-online-privacy

SUGAWARA, Takeshi, BENJAMIN, Cyr; RAMPAZZI, Sara; GENKIN, Daniel; FU, Kevin. Light Commands: **Laser-Based Audio Injection Attacks on Voice-Controllable Systems**. USENIX Association, 2020. Disponível em: https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara

ALENCAR, Antônio Juarez; SCHMITZ, Eber Assis; CRUZ, Leôncio Teixeira. **Assistentes Virtuais inteligentes:** Conceitos e estratégias. Google Books, 2013. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Wd4-AgAAQBAJ&oi=fnd&pg=PA1&dq=assistentes+virtuais&ots=2nYGLeneZZ&sig=5GJUHT_ugZl6ehazygXOufQtLM4#v=onepage&q=assistentes%20virtuais&f=false

NESI, Paolo; PANTALEO, Gianni; SANESI, Gianmarco. **A Hadoop based platform for natural language processing of web pages and documents**. Science Direct, 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1045926X15000749

AMAZON faz acordo para encerrar casos sobre espionagem de 81 mulheres e coleta de dados de crianças. O Globo tecnologia, 2023. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2023/06/amazon-faz-acordo-para-encerrar-casos-sobre-espionagem-de-81-mulheres-e-coleta-de-dados-de-criancas.ghtml

M., Febna V. **Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention.** Beagle security, 2020. Disponível em: https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html

DolphinAttack. Ubiquitous System Security Lab., 2017. Disponível em: https://www.usslab.org/projects/DolphinAttack/DolphinAttack.html

Finkelstein, M. Eugenia, Finkelstein, Claudio. **Privacidade e Lei Geral de Proteção de Dados Pessoais**. Revista de Direito Brasileira, 2020. Disponível em: https://indexlaw.org/index.php/rdb/article/view/5343/4545