Desafios da Privacidade nos Assistentes Virtuais Pessoais

Diana Silva[1], Mariana Malta[1,2,3] e Paulo Vasconcelos[1,2]

[1] ISCAP, Politécnico do Porto

[2] CEOS.PP, Politécnico do Porto

[3] Centro Algoritmi, Universidade do Minho

Resumo

Este artigo apresenta os desafios de privacidade existentes na utilização de dispositivos de assistentes virtuais pessoais.

Como tal, foi realizada uma revisão de literatura utilizando as seguintes bases bibliográficas: EBSCOhost e Google Scholar (Google Académico).

Constatou-se que existem vários riscos na utilização de dispositivos com assistentes virtuais pessoais, os quais podem ser desencadeados por vários motivos, desde falhas mecânicas; falhas de software; falhas na *cloud*, nomeadamente na conexão do dispositivo à Internet; falta de meios de autenticação e autorização fortes; falta de conhecimento e consciencialização dos utilizadores para os perigos e falta de transparência das empresas com os seus clientes na forma como são tratados e armazenados os seus dados e informações privadas.

Em termos de implicações práticas, foi importante identificar que estratégias, comportamentos e atitudes é necessário implementar para superar os desafios apontados pelos autores identificados ao longo do documento.

Palavras-chave: privacidade, inteligência artificial, assistente virtual pessoal, utilizador, riscos, desafios

Abstract

This article presents the privacy challenges that exist in the use of personal virtual assistant devices.

For this purpose, a literature review was conducted using the following bibliographic databases: EBSCOhost and Google Scholar (Google Scholar).

It was found there are several risks in using devices with personal virtual assistants, which can be triggered for various reasons: from mechanical failures; software failures; cloud failures, namely in connecting the device to the Internet; lack of strong authentication and authorisation means; lack of knowledge and awareness of users to the dangers and lack of transparency of companies with their customers in the way their data and private information are handled and stored.

In terms of practical implications, it was important to identify what strategies, behaviours and attitudes need to be implemented to overcome the challenges identified by the authors throughout the document.

Keywords: privacy, artificial intelligence, personal virtual assistant, user, risks, challenges

Introdução

A **Internet das Coisas** (**IoT,** do inglês **Internet of Things**), segundo a visão de Ishii (2019) é a área que se refere a "coisas", tais como dispositivos ou sensores, que se ligam, comunicam e transmitem informações com outros aparelhos ou entre si, através da Internet. Estes dispositivos vão além dos computadores, smartphones ou tablets.

Dentro da área de **IoT**, existe uma área especifica que é a **Inteligência Artificial** (**IA**). A **IA** é considerada como um "sistema de processamento de informações, que produz resultados de forma idêntica ao processo do pensamento do ser humano, seja na aprendizagem, na tomada de decisão ou na resolução de problemas. Isto faz com que a Inteligência Artificial desenvolva sistemas capazes de lidar com os problemas de maneira semelhante à lógica do ser humano" (Pereira, 2021, p.11).

Para desenvolver conhecimento e comunicação com as pessoas reais, a **IA** tem alguns componentes que completam o seu processo. Em primeiro lugar, existe o que se chama de **Aprendizagem Máquina** (**ML,** do inglês **Machine Learning**). O **ML** pode ser definido como "qualquer metodologia e conjunto de técnicas que encontra novos padrões e conhecimentos nos dados, e, por conseguinte, gera modelos (por exemplo, perfis) que podem ser utilizados para fazer previsões eficazes sobre os dados" (Ishii, 2019). Numa linguagem corrente, Machine Learning traduz-se no facto de a máquina ser capaz de aprender e desenvolver essa aprendizagem ao longo do tempo.

Em segundo lugar, há o que se chama de **Processamento Natural da Linguagem** (**NPL,** do inglês **Natural Processing Language**). O **NPL** é uma área de investigação e aplicação que explora como os computadores podem ser usados para compreender e manipular textos ou discursos em linguagem natural para fazer algo útil (Ishii, 2019). Portanto é o processo através do qual se realizam interações entre humanos e máquinas, de forma que a linguagem humana seja percetível para a máquina e vice-versa. O NPL envolve, essencialmente, a análise do campo lexical e semântico da linguagem (Singh e Mishra, 2021).

Os **Assistentes Virtuais Pessoais (AVP)** são equipamentos que "possuem componentes de software com personalidade, os quais suportam a integração natural de emoções, e usam, principalmente, interfaces de voz para interagir com os seus utilizadores. Baseiam a sua comunicação numa linguagem natural, como forma de simular o discurso humano e podem estar presentes em computadores e telemóveis" (Rawassizadeh et al., 2019). No entanto, também existem dispositivos próprios, chamados Assistentes Pessoais para Casas Inteligentes (SPA do inglês Smart Home Personal Assistants) concebidos pelas principais marcas no mercado, tais como: a Amazon, a Google e a Apple, para uso doméstico (Lopatovska et al., 2020). 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 (Abdi et al., 2021).

Este artigo tem como objetivo fazer um levantamento dos desafios para a privacidade dos utilizadores que possuem dispositivos de AVP, quer haja interação ou não com os mesmos.

A análise e informação apresentada no presente artigo foi concebida através da pesquisa e do estudo da literatura existente nas diferentes temáticas abordadas, através do acesso a bases de dados bibliográficas.

O resto do artigo está organizado da seguinte forma: a primeira secção apresenta a abordagem metodológica realizada no estudo, já a segunda secção apresenta uma contextualização teórica, onde são apresentados os desafios da privacidade nos dispositivos de AVP e a perspetiva da Europa em relação aos desafios da privacidade na IA. Finalmente o artigo termina com uma breve discussão e uma conclusão.

Abordagem Metodológica

Foi realizada uma revisão sistemática da literatura com o intuito de compreender conceitos chave da área da IA e dos AVP, de modo a se identificar os desafios que se colocam na proteção de dados no uso dos AVP's. Algumas das questões que se pretende responder são:

1. Conferem os dispositivos AVP proteção aos dados pessoais dos utilizadores?

Pretende-se compreender se os dados pessoais dos utilizadores deste tipo de tecnologia de IA, estão suficientemente protegidos ou não.

2. Quais os riscos relativos à privacidade do utilizador dos AVP podem ser desencadeados com o uso destes dispositivos?

Pretende-se enumerar os vários riscos que podem advir da utilização deste tipo de aparelhos.

3. Qual a perspetiva da União Europeia em relação a esses mesmos desafios na proteção dos utilizadores contra fugas de informações privadas?

Pretende-se perceber qual a perspetiva da União Europeia sobre a IA e o que pretende implementar para aumentar a privacidade e segurança dos cidadãos europeus.

As bibliotecas digitais usadas para a recolha dos documentos científicos foram a EBSCOhost e o Google Scholar (Google Académico). A pesquisa foi realizada desde novembro de 2021 a maio de 2022 e restringiu-se ao período de tempo ente 2012 a 2022.

A pesquisa inicial incluiu os seguintes termos: “artificial intelligence” “and” “virtual assistant” - 146 resultados (apenas foram consideradas os artigos de revistas académicas - EBSCOhost) e 467 resultados (apenas foram consideradas os artigos de revisão - Google Scholar); “artificial intelligence” “and” “personal virtual assistant” – 77 resultados (apenas foram consideradas os artigos de revistas académicas - EBSCOhost) e 6 resultados (apenas foram consideradas os artigos de revisão - Google Scholar).

Numa pesquisa posterior, foram analisados outros termos, tais como: “privacy” “and” “personal virtual assistant” – 27 resultados (apenas foram consideradas os artigos de revistas académicas - EBSCOhost) e 4 resultados (apenas foram consideradas os artigos de revisão - Google Scholar); “privacy” “and” “personal assistant” – 67 resultados (apenas foram consideradas os artigos de revistas académicas - EBSCOhost) e 575 resultados (apenas foram consideradas os artigos de revisão - Google Scholar); “privacy” “and” “smart home” “and” “personal assistant” – 2 resultados (apenas foram consideradas os artigos de revistas académicas - EBSCOhost) e 130 resultados (apenas foram consideradas os artigos de revisão - Google Scholar); “europe” “and” “artificial intelligence” – 422 resultados (apenas foram consideradas os artigos de revistas académicas - EBSCOhost) e 17 100 resultados (apenas foram consideradas os artigos de revisão - Google Scholar).

Os termos também foram procurados em língua portuguesa, no entanto, deu-se preferência à língua inglesa para a apresentação de um maior número de resultados.

Para além dos artigos e livros mencionados, também foram analisadas noticias, nomeadamente as que se encontravam em alguns dos artigos analisados e que tinham importância para a contextualização do tema. Foram considerados relevantes para o estudo, cerca de 12 artigos,

pois foram os apresentaram as melhores informações para dar resposta às questões de investigação definidas.

Enquadramento Teórico

Dispositivos de AVP

Na figura 1 apresentam-se alguns dos dispositivos AVP que podem ser encontrados no mercado, nomeadamente, o Apple Homepod, equipamento da marca Apple; o Google Home, equipamento da marca Google; e o Amazon Echo e o Echo Look, ambos equipamentos da marca Amazon.

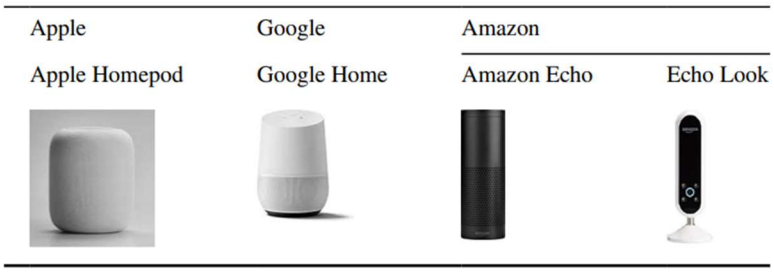

Figura 1 Marcas e Dispositivos AVP (Yang e Lee, 2019)

Estes dispositivos, tal como outras tecnologias, apresentam potencialidades, como por exemplo, tornar o acesso a diversas informações mais rápido e cómodo, mas também riscos que podem surgir através do seu uso. Os desafios encontrados pelos vários autores analisados são enumerados a seguir e que apontam quais as causas e as consequências que podem surgir na utilização destes dispositivos.

Desafios da Privacidade nos Dispositivos de AVP

Rawassizadeh et al. (2019) referem no seu estudo que 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 AVP encontram-se nas residências dos utilizadores. Esta recolha de dados, segundo Bolton et al. (2021), pode traduzir-se numa gravação das conversas do utilizador sem a sua permissão ou conhecimento. Isto pode acontecer, devido ao facto dos dispositivos AVP estarem sempre ligados à internet e os dados serem armazenados na *cloud*, havendo por isso um maior risco de ciberataque ou falha mecânica (Rawassizadeh et al., 2019).

No seguimento dessa ideia, Chung e Lee (2018) apresentam a sua visão. Estes autores realizaram no seu estudo uma experiência com um dispositivo da Alexa, assistente pessoal da Amazon. O foco foi a ***cloud*** deste AVP, sítio virtual onde se encontram muitos dados, os quais estão localizados de forma central num único ponto, que é na arquitetura dos AVP's (Modi et al. 2013). A **arquitetura dos AVP's** é definida como o processo de funcionamento dos assistentes virtuais pessoais, desde o momento em que é feita uma pergunta ou dada uma instrução, até ao momento em que o AVP a realiza (Modi et al., 2013).

Portanto, os autores Chung e Lee (2018), constataram que, em caso de ciberataque à ***cloud*** desse equipamento, os hackers conseguiriam ter acesso ao histórico detalhado dos serviços proporcionados por esse software, assim como, às informações pessoais, aos interesses e aos padrões de vida do utilizador em estudo. Neste caso, não só se poderiam desencadear importantes implicações e ameaças à privacidade dos utilizadores, assim como, dos fornecedores deste tipo de serviço.

Outro aspeto importante no campo dos desafios da privacidade, é a falta de consciencialização dos utilizadores em relação aos potenciais perigos que o uso dos AVP's acarreta, assim como, uma falta de conhecimento em relação ao uso dos seus dados em diferentes contextos (Cunneen et al., 2020). Isto sucede, porque muitas vezes as empresas não são transparentes na forma como recolhem e armazenam os dados dos seus clientes (Bolton et al., 2021). Como consequência, poderá crescer a falta de confiança dos utilizadores nas empresas que comercializam este tipo de serviços e dispositivos (Rawassizadeh et al., 2019).

Também Edu et al. (2020) referem no seu estudo vários desafios que podem comprometer a segurança e privacidade dos utilizadores. Começam por falar do nível de **autenticação** nos dispositivos de AVP. Explicam que a mesma é feita através do uso de palavras de ativação que são reconhecidas pelo aparelho. O utilizador tem a opção de selecionar uma palavra de ativação de um conjunto de opções predefinidas no software. Com este tipo de ativação, torna-se fácil que um hacker possa intervir no sistema. Apontam também que o facto de os AVP não disporem de outras formas adicionais de autenticação, pode fazer com que o dispositivo aceite qualquer instrução, após a ativação da palavra escolhida. Portanto, pode ser fácil para qualquer pessoa próxima do dispositivo ativá-lo.

Depois mencionam a questão da **ligação do dispositivo com a Internet**. O facto de estar sempre ligado ao mundo digital e a ouvir os discursos do utilizador, faz com que esteja constantemente a aguardar pela palavra de ativação definida, logo pode apresentar importantes

preocupações de segurança e privacidade. O que pode acontecer é a palavra de ativação ou qualquer outra palavra foneticamente semelhante ser mencionada, de forma acidental, o que colocará os assistentes a gravar o seguimento da conversa. Posteriormente essa conversa será partilhada com a Internet, afetando assim a privacidade dos utilizadores quando estão em causa informações confidenciais ou sensíveis. Tal foi o que aconteceu, em 2018, quando a conversa de um casal foi acidentalmente gravada e enviada para um dos seus contactos[1]. O dispositivo em questão pertence ao AVP Alexa.

No que diz respeito ao **pagamento de compras**, Edu et al. (2020) informam que os sistemas dos dispositivos dos AVP podem suportar vários pedidos online e, como tal, é cada vez mais um desafio implementar medidas de segurança adequados a esta funcionalidade. Por exemplo, as pessoas que dispõem da Alexa, têm a opção de definir um código PIN de quatro dígitos para confirmar os seus pedidos de compra. No entanto, os autores perceberam que mesmo com a opção de PIN ativada, esse é um mecanismo de bloqueio vulnerável, pois a Alexa permite duas tentativas de PIN antes do bloqueio do processo de compra. Após essas duas tentativas, o utilizador tem de reiniciar todo o seu pedido outra vez. No entanto, no momento do estudo, não havia restrições ao número de vezes que uma pessoa podia tentar fazer um pedido após cada bloqueio. Este exemplo elucida para o facto de que se alguém tentar fazer uma compra, pode inserir várias combinações de códigos PIN diferentes, até efetivamente conseguir efetuar o pedido através do dispositivo de outra pessoa, o que acarreta grandes lacunas na segurança das compras online.

Outro aspeto a considerar é o **acesso de terceiros aos dispositivos AVP** (Edu et al., 2020). Este desafio**,** que em muito vai ao encontro dos problemas apontados anteriormente, diz respeito à proteção das informações dos utilizadores por parte das empresas detentoras de AVP's, das empresas que desenvolvem o seu software, das empresas que desenvolvem os dispositivos inteligentes e de todos aqueles que têm acesso direto a qualquer parte do processo desencadeado por um assistente virtual pessoal, de terceiros que não poderiam ter acesso a nenhum desses dados. Como em todos os outros serviços em *cloud*, a questão apresentada pelos autores fala sobre como os dados recolhidos por estes aparelhos de IA são partilhados com terceiros, assim como, sobre que

[1] Horton, Helena (2018, 25 de maio) "Amazon Alexa Recorded Owner's Conversation and Sent to "random" Contact, Couple Complains". The Telegraph. https://www.telegraph.co.uk/news/2018/05/25/amazon-alexa-recorded-owners-conversation-sent-random-contact/

tipo de mecanismos de controlo podem ser implementados para proporcionar mais segurança aos utilizadores.

Para os autores Edu et al. (2020) importa salientar também que os dispositivos de AVP, podem ainda ser responsáveis por fazer a ligação com outros **dispositivos inteligentes** que podemos encontrar numa **Casa Inteligente** (em inglês ***Smart Home***). Também esses eletrodomésticos podem ser considerados um ponto de acesso para hackers. Ao violar o acesso ao sistema é dada permissão não só para que os invasores controlem uma ampla variedade de dispositivos todos ligados entre si, assim como, terem acesso a vários dados.

Por último, um problema que já foi apontado por Bolton et al. (2021), a **falta de transparência das empresas com os utilizadores**. Edu et al. (2020) vêm completar com a sua visão, no que diz respeito ao facto de que, muitas vezes essas empresas deixam os seus funcionários ouvir as conversas gravadas dos seus clientes, como um processo crítico de avaliação do sistema de reconhecimento de voz do AVP que comercializam[2]. Isto acontece mesmo quando não existe nas suas declarações de privacidade o objetivo de utilizar as gravações dos seus clientes dessa forma, nem que às mesmas será conferido o anonimato. Os autores ainda mencionam informações sobre o campo do **armazenamento dos dados**, onde remetem o seu estudo para a exclusão incompleta dos dados dos clientes da *cloud* dos AVP. Esta situação pode permitir que as empresas desses dispositivos continuem a deter, intencionalmente ou acidentalmente, os dados privados das pessoas, mesmo depois de terem sido eliminados.

A Europa e os Desafios da Privacidade na IA

Como forma de se tentar minimizar e solucionar todas estas questões da invasão da privacidade das pessoas que confiam nas empresas e nos seus serviços ou produtos de AVP, é importante perceber se os países, mais precisamente os Estados-Membros da União Europeia, e o próprio Parlamento Europeu, demonstram vontade em que tal processo seja desenvolvido.

O autor Justo-Hanani (2022) afirma que o facto de haver uma potencial violação dos direitos fundamentais dos cidadãos e dos negócios associados a este tipo de sistemas, no que diz respeito à segurança, às questões de preconceito, à desigualdade e à privacidade, são motivos suficientes para

[2] Picchi, Aimee. (2019, 11 de abril) “Amazon Workers are Listening to What You Tell Alexa”. CBS News. https://www.cbsnews.com/news/amazon-workers-are-listening-to-what-you-tell-alexa/

a União Europeia tomar medidas. Como tal, foi surgindo uma grande preocupação em avançar com a regulamentação dos mercados digitais, incluindo o setor da IA.

Para isso, em 2020, a Comissão Europeia, realizou uma grande reforma através do chamado *White Paper*, onde se proponham políticas para regulamentar a IA, com foco em reforçar o controlo deste setor e garantir uma abordagem ética centrada no ser humano quando este usa produtos ou serviços dessa natureza. No seguimento desse documento, surgiu em 2021, o *Artificial Intelligence Act*, onde havia o desejo de serem implementadas regras nos sistemas de IA e a integração das mesmas no quadro legislativo existente na União Europeia (Regulamento Geral para a Proteção de Dados - RGPD).

No entanto, uma das grandes preocupações apontadas pelos Estados-Membros é o facto de que, a regulamentação possa vir a ser demasiado restritiva ao ponto de dificultar indevidamente o desenvolvimento tecnológico ou de aumentar o custo de criar soluções de IA no mercado. Como tal, será importante ter em conta medidas que resolvam os riscos encontrados, mas ao mesmo tempo não prejudiquem os negócios (Justo-Hanani, 2022).

Discussão

Tal como já foi mencionado acima, as questões de investigação que se pretendia responder, estavam relacionadas com o facto de se desejar saber o nível de proteção conferido pelos dispositivos AVP aos seus utilizadores, que tipo de riscos podem ser desencadeados desse uso e o que a União Europeia desejar implementar para regulamentar de forma mais eficaz e precisa a área da IA.

Tanto quanto é nosso entendimento, depois de todos os desafios apresentados pelos vários autores, irá ser necessário encontrar mais e melhores soluções para mitigar os riscos que existem e que poderão vir a existir no futuro, devido ao uso dos dispositivos AVP.

As várias visões demonstram que qualquer funcionalidade dos AVP's apresenta formas de intrusão na esfera privada das pessoas, o que nos pode fazer questionar se os dispositivos AVP poderão vir a proporcionar mais privacidade no futuro. A União Europeia já demonstrou querer desenvolver novas regras e ações não só para incentivar o investimento das empresas europeias em sistemas, softwares e dispositivos de IA, mas principalmente, para conseguirem que os Estados-Membros proporcionem maior proteção de dados e privacidade aos utilizadores.

Será ainda necessário haver um equilíbrio entre a inovação e a proteção, para que os negócios se possam desenvolver, pois a União Europeia quer acompanhar o desenvolvimento

tecnológico mundial, mas sempre tendo em conta, tal como já é conhecido deste continente, a defesa e preservação dos direitos humanos.

Conclusão

O propósito deste artigo, foi perceber quais os riscos que podem existir quando os dispositivos AVP são utilizados. Este processo de interação homem-máquina é efetuado dentro do espaço habitacional do cidadão, o qual pode possuir uma Casa Inteligente ou não.

Constatou-se que existem vários riscos, os quais podem ser desencadeados por vários motivos, desde falhas mecânicas, falhas de software, falhas na cloud (conexão do dispositivo à Internet), falta de meios de autenticação e autorização fortes, falta de conhecimento e consciencialização dos utilizadores para os perigos e falta de transparência das empresas com os seus clientes na forma como são tratados e armazenados os seus dados e informações privadas.

É notório que os assuntos segurança, privacidade e dispositivos AVP têm cada vez mais importância para o futuro e que terá de haver um grande investimento por parte dos países e das empresas em formas de proteger as informações e dados partilhados através destas tecnologias. De relembrar que não só as pessoas individuais podem ser prejudicadas, mas também as pessoas coletivas, em especial as empresas que comercializam este tipo equipamentos e desenvolvem o seu software. Como tal, há que assegurar que a implementação e o uso de sistemas de IA não afetam negativamente, quer os negócios, quer os seus clientes.

Em termos de limitações ao estudo, uma das dificuldades encontradas, foi tentar recolher informação sobre todos os riscos de privacidade que existem, pois, as tecnologias IA estão em constante mudança, assim como, são desencadeados todos os dias novos ataques aos dados pessoais e aos dados das empresas. Como tal, é difícil comprovar que todos os desafios de privacidade existentes até ao momento, foram aqui apresentados.

Para terminar, no que diz respeito às perspetivas de investigação futuras, será perceber a literacia digital dos cidadãos europeus ao nível da IA; perceber como e onde são armazenados atualmente os dados dos vários dispositivos AVP disponíveis na Europa; perceber também se as políticas de privacidade de cada AVP estão em conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e com o novo Regulamento da Inteligência Artificial (2021) idealizado pelo Parlamento Europeu, e ainda perceber que soluções, para além de leis e regulamentos, podem ser adotadas para reverter as várias situações de perigo enumeradas ao longo do trabalho realizado.

Referências

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021, May). Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1-14). https://dl.acm.org/doi/abs/10.1145/3411764.3445122

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

Chung, H., & Lee, S. (2018). Intelligent virtual assistant knows your life. *arXiv preprint arXiv:1803.00466.* https://arxiv.org/abs/1803.00466

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

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2020). Smart home personal assistants: a security and privacy review. *ACM Computing Surveys (CSUR)*, *53*(6), 1-36. https://doi.org/10.1145/3412383

Horton, Helena (2018, 25 de maio) "Amazon Alexa Recorded Owner's Conversation and Sent to "random" Contact, Couple Complains". *The Telegraph*. https://www.telegraph.co.uk/news/2018/05/25/amazon-alexa-recorded-owners-conversation-sent-random-contact/

Ishii, K. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. *AI & Society*, 34(3), 509–533. https://doi.org/10.1007/s00146-017-0758-8

Justo-Hanani, R. (2022). The politics of Artificial Intelligence regulation and governance reform in the European Union. Policy Sciences, 55(1), 137–159). https://link.springer.com/article/10.1007/s11077-022-09452-8

Lopatovska, I., Griffin, A. L., Gallagher, K., Ballingall, C., Rock, C., & Velazquez, M. (2020). User recommendations for intelligent personal assistants. Journal of Librarianship and Information Science, 52(2), 577-591. https://journals.sagepub.com/doi/abs/10.1177/0961000619841107

Modi, C., Patel, D., Borisaniya, B. et al. (2013). A survey on security issues and solutions at different layers of Cloud computing. J Supercomput 63, 561–592. https://doi.org/10.1007/s11227-012-0831-5

Pereira, K. A. B. (2021). Um estudo sobre o uso da Inteligência Artificial nas empresas. http://riu.ufam.edu.br/handle/prefix/5989

Picchi, Aimee. (2019, 11 de abril) “Amazon Workers are Listening to What You Tell Alexa”. CBS News. https://www.cbsnews.com/news/amazon-workers-are-listening-to-what-you-tell-alexa/

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

Singh, U., Mishra, A. – Artificial Intelligence in Robotics and Automation. In Bhargava, C., Sharma P. - Artificial Intelligence: Fundamentals and Applications. Boca Raton: CRC Press, 2021. ISBN 1000406466, 9781000406467. P. 55-71.

Yang, H., & Lee, H. (2019). Understanding user behavior of virtual personal assistant devices. *Information Systems & E-Business Management*, 17(1), 65–87. https://doi.org/10.1007/s10257-018-0375-1