2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC) | 978-1-6654-8186-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/CSCC55931.2022.00039

Virtual Assistants in a Digital Governance Environment

Luís Pimentel[1,2], Arsénio Reis[1,3], Maria do Rosário Matos Bernardo[2], Tânia Rocha[1,3] and João Barroso[1,3]
[1]*Universidade de Trás-os-Montes e Alto Douro*, Vila Real, Portugal
[2]*Universidade Aberta*, Portugal
[3]*INESC-TEC, Pólo de Vila Real*, Vila Real, Portugal

***Abstract*—Technological developments have had a major impact on the intensive use of electronic equipment, networked or connected to the internet, factors that have boosted the emergence and growth of cybercrime. Measures to mitigate and combat the phenomenon, taking into account its complexity and specificity, must involve all public entities with responsibility in the sector, in a global effort to promote digital literacy in the areas of cybersecurity and computer crime prevention. These comprehensive actions should use digital technologies based on artificial intelligence (AI), such as virtual assistants, whose characteristics allow the massification of information transmission, while enhancing the digital inclusion of users. Government entities are engaged in adopting technologies based on chatbots, with their presence in several areas of public administration. Despite the evolution, these resources have not yet been made available by the entities responsible for mitigating computer crime. On the other hand, although there are government programs aimed at increasing the digital skills of citizens, namely regarding the protection of devices, digital content or personal data, they are not designed for the specificities of cybercrime. In this context, a system based on chatbots, implemented in a digital governance context, by law enforcement agencies, with resources shared with other government entities can contribute to the prevention of cybercrime.**

***Index Terms*—Artificial intelligence, Chatbots, Conversational agents, Natural language processing**

I. Introduction

The intensive use of electronic equipment and the wide offer of services provided on internet platforms has led to the emergence of a large number of criminal phenomena, related to cybercrime. Whether through simple actions or more complex schemes, cyberdangers are part of users' daily lives. An adequate awareness of their existence can help these users to adapt their behavior in order to avoid victimization.

If critical thinking and careful analysis of the information present in digital environments can, in some cases, overcome these intellectual challenges, the perception of a large part of computer crimes is more complex. Thus, it is important to acquire concrete knowledge, with a view to promoting digital literacy in the area of cybersecurity and that can guide a diligent behavior in more complex technological environments. It is thus imperative to devise appropriate forms of prevention, particularly with regard to how cybercriminals act and the multiplicity of existing crimes. In this sense, government entities, police forces and judicial authorities should join forces and assume a more active role in promoting users' digital literacy in the area of cybersecurity and cybercrime prevention.

These awareness actions should be comprehensive and equity, using new technologies, which allow the mass transmission of massify the transmission of reliable knowledge. A technological system based on chatbots can contribute, in an efficient and comprehensive way, to the resolution of a persistent problem, increasingly present in society.

II. Related work

The conception and implementation of technological systems, when intended for a diverse target audience, should have appropriate information channels, associated with comprehensive means of dissemination, as is the case of chatbots.

In formal learning environments several factors that contribute to digital literacy are mentioned, with different origins, namely in continuous learning processes, in the experience, in social environments, in the use of serious games or through interaction with chatbots. [1]

On the other hand, several advantages can also be mentioned in the use of these virtual assistants, related to the optimization of machine learning algorithms, the reaction speed, the standardization and universality of the information provided, the multiple configuration capacity (depending on the target audience), the interaction by text or voice and the possibility of complementing the computer systems with processes to analyze their effectiveness. [1]

A. Chatbots and digital governance

The digital transformation, operated in many sectors of public administration, has been reflected in the implementation of innovative technologies, based on AI, as well as in the approval of government programs promoting digital skills of citizens.

Virtual assistants, in this case chatbots, are currently seen as a suitable means of promoting communication between government entities and citizens [2], in several areas of public interest. Some of these implementations have taken place in central administration, through the well-known Simplex program [3]. In order to boost customer service and information provision processes, chatbots are used in the institutional websites of the General Directorate of Economic Activities (DGAE) [4] and General Directorate of the Consumer (DGC) [5]. Likewise, at local government level, to promote communication with citizens, chatbots were placed in some City

978-1-6654-8186-1/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCC55931.2022.00039

Councils' websites, such as the municipalities of Lisbon [6], Murça [7], Vimioso [8] and Mirandela [9].

In this frame, it is important to mention that the websites of entities with legal powers to fight cybercrime, whether the National Center for Cybersecurity (CNCS) [10], the Judicial Police (PJ) [11] or the Cybercrime Office of the Attorney General's Office (PGR) [12], do not have any virtual assistants, namely chatbots.

III. Related Work

The conception and implementation of technological systems, when intended for a diverse target audience, should have appropriate information channels, associated with comprehensive means of dissemination, as is the case of chatbots.

In formal learning environments several factors that contribute to digital literacy are mentioned, with different origins, namely in continuous learning processes, in the experience, in social environments, in the use of serious games or through interaction with chatbots. [1]

On the other hand, several advantages can also be mentioned in the use of these virtual assistants, related to the optimization of machine learning algorithms, the reaction speed, the standardization and universality of the information provided, the multiple configuration capacity (depending on the target audience), the interaction by text or voice and the possibility of complementing the computer systems with processes to analyze their effectiveness. [1]

A. Chatbots and digital governance

The digital transformation, operated in many sectors of public administration, has been reflected in the implementation of innovative technologies, based on AI, as well as in the approval of government programs promoting digital skills of citizens.

Virtual assistants, in this case chatbots, are currently seen as a suitable means of promoting communication between government entities and citizens [2], in several areas of public interest. Some of these implementations have taken place in central administration, through the well-known Simplex program [3]. In order to boost customer service and information provision processes, chatbots are used in the institutional websites of the General Directorate of Economic Activities (DGAE) [4] and General Directorate of the Consumer (DGC) [5]. Likewise, at local government level, to promote communication with citizens, chatbots were placed in some City Councils' websites, such as the municipalities of Lisbon [6], Murça [7], Vimioso [8] and Mirandela [9].

In this frame, it is important to mention that the websites of entities with legal powers to fight cybercrime, whether the National Center for Cybersecurity (CNCS) [10], the Judicial Police (PJ) [11] or the Cybercrime Office of the Attorney General's Office (PGR) [12], do not have any virtual assistants, namely chatbots.

B. The role of chatbots in preventing computer crime.

Although some software agents are used for illicit or ethically reprehensible purposes, as is the case of social bots, they can also be used in learning environments, more specifically in the promotion of digital literacy in the context of computer crime prevention. Chatbots have been implemented in systems that aim to inform citizens about the various types of computer crime [13], among which, specifically, in order to promote awareness actions among children and young people [14], as well as in relation to various criminal activities that affect adults, including more vulnerable users, such as older people. [15]

C. The trust shown by chatbots

The relevance of using virtual assistants to promote technological systems in digital governance environments is also gauged by the trust that chatbots convey to their users. To this extent, trust is an important attribute for users to rely on a software agent, in order to share personal information, with a given computer system. In an organizational context, trust is characterized by some fundamentals, related to belief, competence and integrity. These attributes, in the case of a careful implementation with respect to performance and content provided, end up also characterizing the chatbots. [16] There has also been an increase of factors related to trust in systems based on chatbots, particularly for its integration in proposals based on blockchain technology, as a factor of security and authentication in the security and authentication factor in the financial transactions sector. [17]

IV. Cybercrime

The intensive use of electronic equipment, networked or connected to the Internet, as well as the specificities of computer crime, have led to a generalized increase in the number of victims, of all ages, social or academic conditions. [18]

A. The rise of cybercrime

According to the Cybersecurity in Portugal, Risks and Conflicts 2020 Report [10], prepared by the National Center for Cybersecurity (CNCS), according to Figure 1, there has been a significant increase in cybercrime over the past few years.

Other government sources, such as the RASI [19], also show this growth trend.

The Annual Report on Internal Security 2020 (RASI) [19], made available by the National Security Office (GNS) shows, according to Figure 2, a significant increase, over the last decade, of cybercrime.

The statistics presented refer only to reports of cybercrime, leaving unaccounted several types of crime, called cyberdependent, concerning criminal activities committed using computer means and that do not fall under the Cybercrime Law.

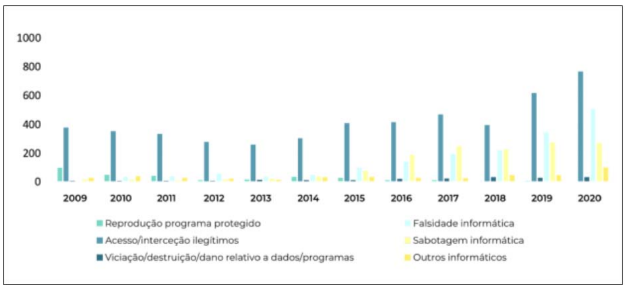

Fig. 1. Cybercrime data (2009 to 2020). Source: Report of Cybersecurity in Portugal - Year 2020 [10]

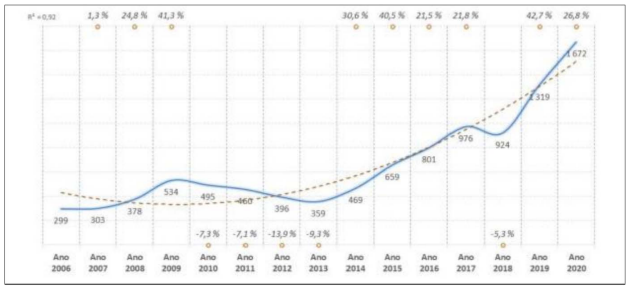

Fig. 2. Cybercrime data (2009 to 2020). Source: Annual Homeland Homeland Security (RASI) - Year 2020 [19].

B. Incidence of cybercrime

In many situations, sophisticated fraudulent schemes, as well as as well as the advanced technological means employed in the processes make it difficult to adequately protect victims and electronic devices. electronic devices. On the other hand, there are victimization factors that that can be perfectly prevented, as is the case of social engineering social engineering, the inadequate protection of devices and services and services, as well as the existence of simple distractions.

1) The vulnerability of some victims: Not all users are familiar with and equipped with digital skills in the area of cybersecurity. The diversity of computer crime methodologies means that some are unable to adapt to the new technological reality, so it is essential to promote their digital literacy in a cybersecurity context, using, for that purpose, adequate accessibility factors.

Regarding young people and children, there is already some awareness on the part of parents and school environments, which, through simple parental supervision or sensitization, end up by mitigating mitigate some of the existing risks.

The problem arises when certain types of crime reach incautious and more vulnerable users, unaware often unaware of the simple forms of criminal action or of the basic basic norms of cybersecurity.

In this context, one of the segments of the population that is vulnerable relates to users who do not have any digital any digital skills, who are older [20] or suffer from who suffer from any form of disability, either motor or cognitive motor or cognitive disabilities [21].

This reality includes a multiplicity of criminal activities that most affect this type of victims, such as financial fraud [22], dating fraud (romance scam) [23], e-commerce fraud [21], financial fraud [24], involvement, even if negligent, in money laundering crimes (money mule) [25], as well as a variety of phishing situations (e-mail, SMS or social networks) [26].

C. Digital Literacy

In general, there are four main pillars that constitute digital literacy, related to digital skills, digital culture, digital ethics and digital security [27]. Its development largely depends on the involvement of education-related entities, community organizations, government institutions, not only in the form of socialization, but also related to other educational activities, such as seminars or group discussions. Many of the digital skills involve evaluating the information present in digital and technological environments, in a critical and effective way, such as such as the ability to use social media.

D. The importance of digital literacy

Literacy, in a pre-digital context, essentially refers to actions related to reading and writing, however, the concept goes far beyond the technical dimension and reaches the ability to understand, contextualize, and be persuasive. It manifests itself through a symbiosis of technical, social and ethical skills and considerations, possessing a permanent capacity for adaptation and evolution [28].

Currently, users interact permanently with electronic equipment in a digital context, whether to access social networks, surf the Internet, shop online or simply in leisure activities. Therefore, they have to develop new forms of literacy in the digital world, in order to adapt to the new technological realities.

According to CNCS [10], education and awareness about cybersecurity-related phenomena are one of the fundamental pillars for the preventive component of this phenomenon. They have the ability to influence attitudes and change behavior, given the sharp growth of cybercrime.

V. Digital Governance

Given the importance of digital environments namely in cybersecurity issues, there has been the implementation of government programs government programs, considered strategic, in the context of digital as strategic, in the context of digital governance.

A. Digital Skills Programs

Government entities have resorted to measures to promote citizens' digital competencies. One of the programs refers to the National Digital Skills Initiative e.2030, Portugal (INCoDe.2030) [29], approved by the Resolution of the Council of Ministers No. 26/2018, of March 8, whose main goal is to respond to the diagnosed needs on digital skills of the Portuguese population.

The Dynamic Reference Framework of Digital Competence (DDRSCF) was also created, with a view to the adoption by

Portugal of the European Framework of Digital Competence for Citizens (DigComp 2.1) [30], especially with regard to the concepts referring to various levels of complexity and autonomy of users, in the context of digital skills.

Although cybersecurity and cybercrime are not directly addressed by these measures, the DCFR refers to the concrete need to implement measures that promote digital competencies in several areas of security and privacy, namely regarding device protection, digital content or personal data.

B. The entities involved in the prevention and fighting computer crime

Possible measures to be implemented in the area of cybersecurity and computer crime prevention, taking into account the specificity of the matter, should not be exclusively limited to the central government. Other public entities, with competence in certain areas of cybercrime mitigation, should contribute with concrete initiatives to combat the phenomenon. These preventive awareness strategies must be framed in high standards of knowledge, through a coordinated involvement.

The Polícia Judiciária (PJ) has reserved powers, which cannot be may not be deferred to other police forces, for the investigation of ”computer and investigation of ”computer crimes and crimes committed with the use of computer technology” [31].

In turn, the National Center for Cybersecurity (CNCS), integrated and under the dependence of the National Security Office (GNS), ”has the mission of contributing so that the country uses cyberspace in a free, reliable and safe way, through the promotion of the continuous improvement of national cybersecurity and international cooperation, in conjunction with all competent authorities, as well as the implementation of measures and tools necessary to anticipate, detect, react and recover from situations that, given the imminence or occurrence of incidents or cyber attacks, jeopardize the operation of critical infrastructures and national interests” [32].

Regarding judicial authorities, such as the Public Prosecutor’s Office, they also have an active role in coordinating many of the investigations, as well as in preventing computer crime. The Cybercrime Office, coordinates the cooperation of the activity of the Public Prosecutor’s Office in the area of cybercrime, under the direct guidance of the Attorney General’s Office (PGR). This office has as its main function ”the internal coordination of the Public Prosecutor’s Office in this area of crime, specific training on the subject and the generic establishment of communication channels with service providers of access to communication networks, to facilitate their collaboration in criminal investigation” [33].

In line with this framework, it is important to emphasize the importance of police entities, in this case the PJ, taking into account its experience in the investigation of this type of crime. This entity is also endowed with legal powers to determine the most effective ways to combat the phenomenon, determine the best means to develop investigations, as well as implement the preventive actions and implement the preventive actions deemed most appropriate [34].

VI. System for the Prevention of Computer Crime Based on Chatbots

The system now proposed, considered feasible, fits perfectly into current digital governance strategies and intends to fill a gap in existing policies for the criminal prevention criminal prevention of computer crime.

A. System Architecture

The architecture of this system, as shown in Figure 2, is based on development of a chatbot on the website of the promoting police entity to disseminate information appropriate to the purpose outlined purpose, concerning the prevention of computer crime.

The contents to be disseminated are developed by this police with the involvement of other government agencies with responsibility in the area, i.e. the CNCS and the Office of Cybercrime of the OPG. PGR.

Besides the intrinsic issue of factors that drive accessibility already accessibility already mentioned, the content produced should also should be present on the institutional website of the promoting entity.

This information, deemed reliable, constitutes a solid solid knowledge base that will feed the source of information for all virtual assistants.

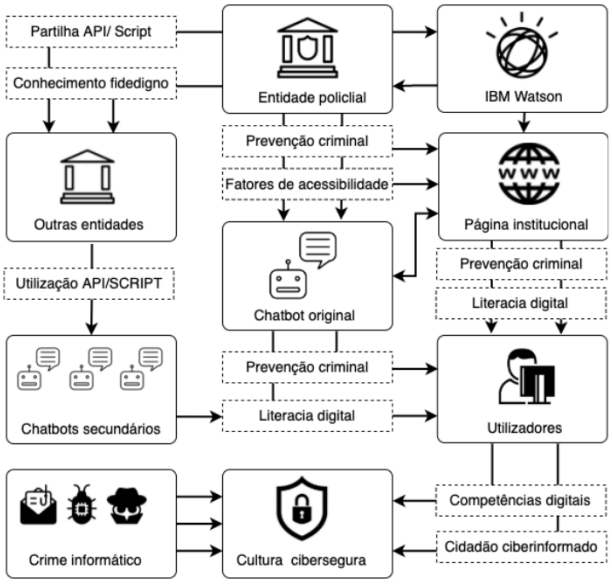

Fig. 3. Diagram of the system for computer crime prevention, based on chatbots.

One of the innovative aspects of the system relates to the sharing resources between state agencies. Parallel to the main chatbot, other governmental government entities can easily integrate the same technology by sharing resources present

in the original instance of the virtual instance of the virtual assistant, either by API or Srcipt, thus massifying the the desired effect.

B. Implementation and technical solutions

Some efficiency and security issues should be evaluated when implementing the system. The nature of the data and content to be shared do not have associated confidentiality attributes, and therefore it is deemed appropriate to implement the system in line with the new paradigms of Software as a Service - SaaS, in order to increase the efficiency of the entire project.

There are several technologies and platforms that allow the implementation, configuration and management of virtual assistant resources, as is the case, among others, of IBM Watson Assistant [35], Amazon Lex [36], Amazon Polly [37], Dialogflow (Google) [38], Amelia [39], Nuance [40] or LUIS (Microsoft) [41].

The IBM Watson Assistant [42], present on the IBM Cloud platform, equipped with artificial intelligence, has characteristics that are adequate to the the functionalities to be implemented, namely regarding the configuration of as to the configuration of the respective layout. Its easy integration platforms, either by API or Scipt, its high security and authentication and authentication standards, as well as the possibility of using the use of the base version with 10,000 monthly requests, free of charge requests per month, free of charge, during the testing phase, make IBM Watson Assistant a solution for the initial projection of the system.

C. Chatbots in promoting accessibility

The importance of factors related to accessibility, usability, and user experience, especially with regard to the existence of possible disabilities, even cognitive ones [43], are also considered in the system.

Fig. 4. Mixed layout of the chatbot, with navigation labels and knowledge direction.

Thus, on the one hand, we have the virtual assistants, characterized as an adequate tool for the comprehensive dissemination of information and promoters of digital inclusion, at the same time that it is possible to adapt their own layouts and functionalities to the generality of users. The mixed programming of layouts, associated with a search and visualization interface, without the need to write or use keyboards, enables the use of the system by users who may present eventual difficulties of interaction with computer systems.

In this sense, as shown in Figure 4, there is the implementation of a of a knowledge tree suitable for navigation and knowledge direction through touch (or mouse click), with the use of with the use of labels, adequately structured, in terms of size and structured, in terms of dimension and content, in order to enable the full integration of all users.

VII. Conclusions

Above all, it is important to emphasize the innovative aspect and effective viability of the idealized system, in a context of digital governance context. It would certainly represent an added value in the and importance of promoting concrete measures for digital literacy and literacy and digital skills among citizens, in the area of cyber cybersecurity, with the concrete goal of preventing computer crime, a phenomenon crime, a phenomenon that is growing widely and worryingly in all sectors of society growth in all sectors of society.

As we have seen, the underlying complexity of certain criminal criminal actions calls for greater attention from government authorities, in order to promote authorities with a view to promoting concrete actions. Despite there are some programs that aim to promote digital digital skills among citizens, they do not directly target the phenomena of the phenomena of computer crime. On the other On the other hand, despite the existence of chatbots in several public services public services, either at the central or local government level, this technology technology ends up not being present in the entities with responsibility in mitigating these criminal phenomena.

In this context, the entities responsible, in national territory for cybersecurity and investigation of computer crimes, in this case, the crimes, in this case, the PJ, the CNCS and the Office of Cybercrime of the PGR, have all the conditions, either at the technical or legal level, to contribute to preventive strategies to raise awareness of cybercrime, to contribute to preventive awareness strategies.

To this end, the characteristics listed above about virtual assistants, as well as the virtual assistants, as well as their proven usefulness in the context of e-government context of e-government, make chatbots an option to be taken into the promotion of digital cybersecurity literacy and cybercrime prevention. cybercrime.

Equal access to these resources, by the whole polution, is safeguarded, is safeguarded. Firstly, the use of the chatbots themselves and their configuration, in terms of layouts are attributes considered adequate in factors that promote usability and user experience. On the other on the other hand, there is also the sharing of knowledge and technology necessary for the replication of other virtual assistants, in various government platforms, either by API or by Script.

Thus, we can easily conclude that the idealized system system can contribute to the promotion of a true and universal

digital culture of citizens on the topics of cybersecurity and cybercrime prevention.

ACKNOWLEDGMENT

This work was supported by the RD Project "Continental Factory of Future, (CONTINENTAL FoF) / POCI-01-0247-FEDER-047512", financed by the European Regional Development Fund(ERDF), through the Program "Programa Operacional Competitividade e Internacionalização (POCI) / PORTUGAL 2020", under the management of aicep Portugal Global – Trade Investment Agency.

REFERENCES

[1] A. Kateryna, R. Oleksandr, T. Mariia, S. Iryna, K. Evgen, and L. Anastasiia, "Digital literacy development trends in the professional environment," *International Journal of Learning, Teaching and Educational Research*, vol. 19, no. 7, pp. 55–79, 2020.

[2] A. Androutsopoulou, N. Karacapilidis, E. Loukis, and Y. Charalabidis, "Transforming the communication between citizens and government through ai-guided chatbots," *Government information quarterly*, vol. 36, no. 2, pp. 358–367, 2019.

[3] Simplex. (2021) Assistente virtual simplifica o atendimento a empresas e a consumidores.

[4] "Direção-geral das atividades económicas." [Online]. Available: https://www.dgae.gov.pt/

[5] "Direção-geral consumidor." [Online]. Available: https://www.consumidor.gov.pt/

[6] "Lisboa - municÍpio de lisboa." [Online]. Available: https://www.lisboa.pt/

[7] "Cm murça." [Online]. Available: https://www.cm-murca.pt/

[8] "C.m. vimioso." [Online]. Available: https://www.cm-vimioso.pt/

[9] "Cm mirandela." [Online]. Available: https://www.cm-mirandela.pt/

[10] CNCS. (2021) Relatório Cibersegurança em Portugal – Sociedade 2020.

[11] "Polícia judiciária." [Online]. Available: https://www.policiajudiciaria.pt/

[12] "Gabinetedecibercrime." [Online]. Available: https://cibercrime.ministeriopublico.pt/

[13] E. Adamopoulou and L. Moussiades, "Chatbots: History, technology, and applications," *Machine Learning with Applications*, vol. 2, p. 100006, 2020.

[14] V. Vijayakumar and D. Hari Prasad, "Intelligent chatbot development for text based cyberbullying prevention," *International Journal of New Innovations in Engineering and Technology*, vol. 17, no. 1, pp. 73–81, 2021.

[15] S. Srivastava, K. Srivastava, and N. Arora, "Exploration of a solution-centric crime awareness tool," *International Journal of Computer Applications*, vol. 975, p. 8887.

[16] A. Przegalinska, L. Ciechanowski, A. Stroz, P. Gloor, and G. Mazurek, "In bot we trust: A new methodology of chatbot performance measures," *Business Horizons*, vol. 62, no. 6, pp. 785–797, 2019.

[17] M. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and S. Tarkoma, "Bonik: A blockchain empowered chatbot for financial transactions," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 1079–1088.

[18] S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C. Whybrow, and T. Glenn, "Increasing cybercrime since the pandemic: Concerns for psychiatry," *Current psychiatry reports*, vol. 23, no. 4, pp. 1–9, 2021.

[19] GNS. (2021) RASI - Relatório Anual de Segurança Interna - 2020.

[20] A. Kalache and A. Gatti, "Active ageing: a policy framework," , no. 11, p. 7, 2003.

[21] M. D. Reisig and K. Holtfreter, "Shopping fraud victimization among the elderly," *Journal of Financial Crime*, 2013.

[22] L.-A. Fenge and S. Lee, "Understanding the risks of financial scams as part of elder abuse prevention," *British Journal of Social Work*, vol. 48, no. 4, pp. 906–923, 2018.

[23] J. Huang, G. Stringhini, and P. Yong, "Quit playing games with my heart: Understanding online dating scams," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2015, pp. 216–236.

[24] D. Burnes, C. R. Henderson Jr, C. Sheppard, R. Zhao, K. Pillemer, and M. S. Lachs, "Prevalence of financial fraud and scams among older adults in the united states: A systematic review and meta-analysis," *American Journal of Public Health*, vol. 107, no. 8, pp. e13–e21, 2017.

[25] R. Leukfeldt and E. E. Kleemans, "Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms," in *Criminal networks and law enforcement*. Routledge, 2019, pp. 75–89.

[26] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, and N. Ebner, "Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing," in *Proceedings of the 2017 chi conference on human factors in computing systems*, 2017, pp. 6412–6424.

[27] J. Sandra, "The importance of digital literacy for society 5.0: A phenomenological approach," *Technium Soc. Sci. J.*, vol. 28, p. 849, 2022.

[28] L. Floridi, *The onlife manifesto: Being human in a hyperconnected era*. Springer Nature, 2015.

[29] Conselho de Ministros. (2019) Despacho n.o 1088/2019: Criação do Quadro Dinâmico de Referência de Competência Digital - QDRCD.

[30] M. Lucas e A. Moreira. (2017) Digcomp2.1.

[31] LOIC. (2021) Lei de organização da investigação criminal - Lei n.o 49/2008, de 27 de Agosto.

[32] GNS. (2017) Orgânica do Gabinete Nacional de Segurança - Decreto-Lei n . o 3/2012,de 16 de Janeiro.

[33] PGR. (2011) Procuradoria-geral da república - Despacho de criação Gabinete Cibercrime, de 7 de dezembro de 2011.

[34] L. F. Tatarinova, K. N. Shakirov, and D. V. Tatarinov, "Criminological analysis of determinants of cybercrime technologies," *International Electronic Journal of Mathematics Education*, vol. 11, no. 5, pp. 1127–1134, 2016.

[35] "Virtual agent - ibm watson assistant." [Online]. Available: https://www.ibm.com/cloud/watson-assistant

[36] "Aws lex - amazon web services." [Online]. Available: https://aws.amazon.com/pt/lex/

[37] "Amazon polly." [Online]. Available: https://aws.amazon.com/pt/polly/

[38] "Dialogflow — google cloud." [Online]. Available: https://cloud.google.com/dialogflow

[39] "Amelia, the market-leading conversational ai solution — amelia." [Online]. Available: https://amelia.ai/conversational-ai/

[40] "Nuance - conversational ai for healthcare and customer engagement — nuance uk." [Online]. Available: https://www.nuance.com/en-gb/index.html

[41] "Luis (language understanding) - cognitive services - microsoft." [Online]. Available: https://www.luis.ai/

[42] "Ibm watson assistant - chatbot integrations." [Online]. Available: https://www.ibm.com/products/watson-assistant/integrations

[43] G. C. Vanderheiden and S. L. Henry, "Designing flexible, accessible interfaces that are more usable by everyone," in *Proceedings of the 2003 CHI Conference on Human Factors in Computing Systems (CHI 2018)*, 2003.