International Journal of Human–Computer Interaction

ISSN: 1044-7318 (Print) 1532-7590 (Online) Journal homepage: www.tandfonline.com/journals/hihc20

"The Implementation of Public Chatbots to Raise Awareness of Computer Crime"

Luís Pimentel, Maria do Rosário Bernardo & Tânia Rocha

To cite this article: Luís Pimentel, Maria do Rosário Bernardo & Tânia Rocha (05 Jun 2025): "The Implementation of Public Chatbots to Raise Awareness of Computer Crime", International Journal of Human–Computer Interaction, DOI: 10.1080/10447318.2025.2508302

To link to this article: https://doi.org/10.1080/10447318.2025.2508302

INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION
https://doi.org/10.1080/10447318.2025.2508302

"The Implementation of Public Chatbots to Raise Awareness of Computer Crime"

Luís Pimentel[a], Maria do Rosário Bernardo[b], and Tânia Rocha[c]

[a]Universidade de Trás-os-Montes e Alto Douro, Universidade Aberta, Vila Real, Portugal; [b]CEG-Universidade Aberta, INESC TEC, Lisboa, Portugal; [c]Universidade de Trás-os-Montes e Alto Douro, INESC TEC, Vila Real, Portugal

ABSTRACT

Recent technological advancements have increased computer crime, requiring public authorities to implement structured mitigation strategies. While initiatives exist to improve digital literacy on device security, they must also address the complexities of computer crime. Using Design Science Research, this study investigated the applicability of chatbots to raise awareness of computer crime in a public administration setting. A systematic literature review highlighted the issue's relevance and identified knowledge gaps. A scoping review gathered concepts, methodologies, technologies, architectures, and tools for developing and evaluating an effective chatbot. The design and development phase included a detailed proposal for a sophisticated chatbot architecture. During the demonstration and evaluation phases, the utility of the chatbot was tested in the domain of conversational flow efficiency and usability. The study's primary results and contributions are to assess the chatbot's effectiveness in raising awareness of computer crime on public websites. Future work should focus on implementing the chatbot in the actual context of public administration, proposing a network of specialized conversational assistants, and improving public service interoperability to enhance computer crime awareness.

KEYWORDS

Public administration; evaluation; chatbots; computer crime awareness; development

1. Introduction

The intensive use of electronic equipment and the wide range of services provided over the Internet have led to an increase in cybercrime (ARRS - Slovenian Research, 2022; NCSC, 2022). Through simple actions or more complex schemes, cyber dangers are part of users' lives (Singh, 2011; Weisburd & McEwen, 2015). Although critical thinking or careful content analysis can overcome intellectual challenges, the perception of computer crimes is more complex (Tatarinova et al., 2016). The education and awareness of cybersecurity phenomena are the pillars of its prevention (NCSC, n.d.). Awareness of these phenomena and adequate clarification of the various forms of criminal activity can help adjust behaviors, thus avoiding victimization (Srivastava et al., 2020). Despite government initiatives providing digital skills in security and privacy in Portugal (Presidency of the Council of Ministers, 2018), protecting devices, digital content, and personal data (The Presidency of the Council of Ministers, 2019) does not explicitly refer to awareness of computer crime. In a context of high technological development and growing interaction between government and citizens (Filipe et al., 2012), reflected in innovative public policies (Ubaldi et al., 2019) and the provision of emerging technologies to promote efficient communication, it was essential to assess whether these developments could contribute to mitigating and raising awareness of computer crime. Exploratory research and preliminary literature review processes aimed at identifying emerging IT solutions (artifacts) with the potential, in a public administration (PA) context, to promote communication between the State and the citizens have identified artificial intelligence (AI) (Henman, 2020; Ubaldi et al., 2019) as technology and conversational assistants (chatbots) as a tool (Kumar & Mukund, 2020; Zuiderwijk et al., 2021).

The explorative research also discovers the types of computer crime that occur most frequently and entities that could contribute awareness-raising content for the artifact's knowledge base. Government reports were also researched to address the incidence of computer crime and the types of crime in Portugal. Several organizations in Portugal and the European Union were identified as being dedicated to raising awareness of computer crime and producing awareness-raising content, namely the *Portuguese Association for Victim Support* (PAVS) (APAV, n.d.); the *Portuguese Bank* (PB) (Banco de Portugal, n.d); the *Safe Internet Center* (SIC) (Centro de Internet Segura, n.d); *Deco Protest* (DECO) (DECO PROteste, n.d); the *European Cybercrime Centre* (EC3-Europol) (EC3, n.d); and the *European Union Agency for Cybersecurity* (ENISA) (ENISA, 2024). In the same vein, entities with legal powers related to investigating and mitigating computer crime were identified, namely the *Public Prosecutor's Office* in Portugal (Ministério Público, n.d) and the *Judicial Police* (JP) (Polícia Judiciária, n.d), as well as in

CONTACT Luís Pimentel al75334@alunos.utad.pt Universidade de Trás-os-Montes e Alto Douro (Vila Real), Universidade Aberta (Lisboa), Portugal
Supplemental data for this article can be accessed online at https://doi.org/10.1080/10447318.2025.2508302.

cybersecurity areas related to the *National Cybersecurity Center* (NCC) (Centro Nacional de Cibersegurança, n.d).

Multiple searches were carried out in chatbot development platforms provided by Google (Dialogflow), Microsoft (Azure), and IBM Cloud (Watson Assistant). We took advantage of the free plan and opted for Watson Assistant to implement the artifact architecture.

This study examined the relevance, admissibility, and parameters of using public chatbots to raise awareness about computer crime. In this sense, the primary research question was: "Is it possible to develop an innovative artifact (chatbot) to implement on public administration websites, focusing on citizens aware of phenomena related to computer crime?"

This work is structured in seven sections, including this introduction (section 1), the related work (section 2), the research methodology (section 3), the design and development phase (section 4), the demonstration phase (section 5), the evaluation phase (section 6), and the conclusions (section 7).

2. Related work

There is a significant increase in computer crime (ARRS - Slovenian Research, 2022; NCSC, 2022) which affects victims of all ages and social conditions, with a higher incidence during and after the COVID-19 pandemic (Monteith et al., 2021). Although computer crime has a global dimension and can affect any victim, it mainly affects more vulnerable people unaware of how criminals operate and the basic safety rules when using digital resources. Some of the most vulnerable users, such as older people (Kalache & Gatti, 2003), with possible forms of disability, whether motor or cognitive (Agência para a Modernização Administrativa, n.d), can be victims of a multitude of criminal activities related to: financial fraud (Fenge & Lee, 2018); e-commerce fraud (Reisig & Holtfreter, 2013) with digital payment (Burnes et al., 2017); the participation, even negligently, in money laundering crimes (*money mule*) (Hufnagel & Moiseienko, 2019); or phishing actions (Oliveira et al., 2017). There are situations in which victims are psychologically weakened (Coluccia et al., 2020), especially in cases of victimization by criminal schemes known as *romance scams* (Anesa, 2020; Huang et al., 2015). In this case, the social stigma resulting from financial losses makes the victims feel guilty and ashamed, inhibiting them from seeking help from the police and family (Anesa, 2020). The attributes of anonymity that chatbots can provide help victims.

2.1. Promoting digital skills and competences

In Portugal, some strategic government initiatives provide ordinary citizens with digital skills, which addresses the need to increase their skills in new digital technologies (Presidency of the Council of Ministers, 2018). The *Dynamic Reference Framework for Digital Competence (DRFDC)* (The Presidency of the Council of Ministers, 2019) covers five areas that bring various digital skills to be promoted, like information literacy, communication, citizenship, content creation, security, and privacy, as well as the development of IT solutions. Although it does not focus on computer crime, the DRFDC promotes digital skills in security and privacy concerns, namely the protection of devices, digital content, and personal data (The Presidency of the Council of Ministers, 2019). Education and cybersecurity awareness are fundamental pillars of the prevention component of phenomena related to computer crime (Centro Nacional de Cibersegurança, 2021).

2.2. Emerging technologies in the public sector

The definition of e-government includes digital governance related to the growing technological development and the interactions between government and citizens (Filipe et al., 2012; Ubaldi et al., 2019). Artificial intelligence was recognized as a technology that identifies IT solutions in PA, promoting State communication. Chatbots were identified as tools that could become part of universal awareness-raising actions, using emerging technologies and allowing the massification of reliable content (Osakwe et al., 2021). In the same context of emerging technologies in the public sector, the usefulness of conversational assistants is highlighted, particularly concerning chatbots (Kumar & Mukund, 2020; Zuiderwijk et al., 2021). The digital transformation has led to the creation of IT solutions based on AI, namely chatbots, whose characteristics offer great potential for promoting communication processes between the State and the citizen (Kumar & Mukund, 2020; 2020; Zuiderwijk et al., 2021).

2.3. Conversational assistants (chatbots)

Chatbots are computer programs designed to interact with users in real time using text, voice, or natural language (Hasan et al., 2021). One of the best-known, ELIZA, developed by MIT (Massachusetts Institute of Technology) in 1966, was considered the pioneer in this field (Hasan et al., 2021). Since then, conversational assistants have had various applications in banking, tourism, health, business, education, and financial institutions (Androutsopoulou et al., 2019). According to the general description of chatbots, they have three essential elements: their interface, the natural language processing (NLP) engine, and the knowledge base (Nirala et al., 2022). The interface can be a website, instant messaging, or mobile app. The NLP engine manages the semantic context of conversations. The knowledge base becomes the central core of content that makes interactions possible (Nirala et al., 2022). Considering the knowledge base, there are three main varieties of chatbots: rule-based, retrieval-based, and generative-based (Adamopoulou & Moussiades, 2020; Androutsopoulou et al., 2019). Some studies refer to the benefits of chatbots in the e-government context: AI task improvement (Kumar & Mukund, 2020; Wang et al., 2021); promoting communication processes (Nirala et al., 2022); optimizing its interaction with users (Chaves & Gerosa, 2021) in the context of digital governance (Kumar & Mukund, 2020); the informative capacity (Nirala et al., 2022; Wang et al., 2021); the technological innovation that they represent (Nirala et al., 2022); its great versatility in terms of multiple uses (Kumar & Mukund, 2020; Wang et al., 2021); and the characteristics that promote its user-

centered action (Nirala et al., 2022) leading to their loyalty (Chaves & Gerosa, 2021; Wang et al., 2021). Regardless of their focus in the e-government context, some studies refer to solutions in the awareness of computer crime: through a generalist view of the phenomenon (Hamad & Yeferny, 2020; Khokhawat et al., 2021); in the prevention of cyberbullying (Hari Prasad & Vijayakumar, 2021); collecting data via the dark web (Budiman & Aminanto, 2022); with issues related to cybercrime (Srivastava et al., 2020); in the provision of cybersecurity content via WhatsApp (El Hajal et al., 2021); in training cyber analysts (El Hajal et al., 2021); in the social engineering prevention (Banire et al., 2021); and cybersecurity training in schools (He & Xin, 2021). Given the public websites that can integrate chatbots, it is essential to consider good practices in developing these resources, focusing on accessibility, usability, and user experience. Some innovative techniques, such as architecture, are based on intelligent agents (Hatsue et al., 2000). We can see standards that improve aspects of accessibility on the subject (W3C, n.d.a), defined in the guide U*ser Agent Accessibility Guidelines (UAAG) Overview* (W3C, n.d.b). There is also scientific interest in the impact of chatbots on accessibility issues (W3C, 2021), usability (Borsci et al., 2022), and user experience (Cheng & Jiang, 2020).

2.4. The literature review

The literature review included a systematic literature review (SLR) and a scoping review (SR). The SLR, which adhered to the model proposed by Kitchenham and Charters (Barbara & Stuart, 2007), demonstrated the relevance of the problem and allowed for the identification of knowledge gaps. The SR, following the PRISMA Extension for Scoping Reviews (PRISMA-ScR) guidelines (Tricco et al., 2018), facilitated the identification of concepts, methodologies, technologies, and tools to develop, evaluate, and optimize architectures suitable for the investigation purpose.

2.4.1. Systematic literature review

The SLR (Barbara & Stuart, 2007) supported the objectives and research questions and demonstrated their relevance. The criteria for inclusion and exclusion were designed to encompass primary studies that contribute scientifically, in line with the motivation and goals of this SLR. This study specifically investigates the conceptualization of chatbots in the realm of e-government aimed at preventing and raising awareness of computer crime. Additionally, the research focuses on primary studies published from 2009 onwards 2022. This time-lapse reflects the implementation of Law 109/2009, dated September 15, which pertains to the initial version of the Cybercrime Law in Portugal (Assembly of the Republic, 2009), as well as the year of this research, specifically 2022. This study selection process identified 46 articles that met all criteria (inclusion, exclusion, and quality) and were submitted for data extraction. The final list included articles from various digital libraries: ACM Digital Library (17); DOAJ, Open Trusted (1); IEEE Digital Library (4); MDPI, Social Sciences (1); Science Direct (4), Scopus (10), Springer Link (2); Taylor & Francis Online (2); Web of Science (4); and Wiley Online Library (1). We conducted a narrative synthesis that involved two types of analyses: a description of the selected publications for review and a thematic analysis of these publications in relation to the research questions and the proposed theoretical framework.

The SLR identified data to consider in chatbot proposals: the areas of chatbot implementation in an e-government context (Q1); the attributes of these chatbots within the same e-government context (Q2); the intervention areas of chatbots in raising awareness of computer crime, even if they fall outside the e-government context (Q3); the areas of chatbots' intervention in raising awareness of computer crime, specifically within the context of e-government (Q4); legal documents, standards, or guidelines applicable in Portugal or the European Union regarding emerging technologies in the e-government context (Q6); and web development standards and procedures, particularly for chatbots, concerning user experience within the e-government context (Q7).

Regarding Q1, the SLR identified various areas within public administration where chatbots are implemented, including multiple administrative domains of the public sector (Akkaya & Krcmar, 2019; Androutsopoulou et al., 2019; Aoki, 2020; Stamatis et al., 2020; van Noordt & Misuraca, 2019; Wilson & Marasoiu, 2022); in the health sector (Akkaya & Krcmar, 2019; Aoki, 2020; de Melo & Monteiro, 2021; Nirala et al., 2022; Simonsen et al., 2020; Tao et al., 2019); in the social security sector (Akkaya & Krcmar, 2019; van Noordt & Misuraca, 2022; Vassilakopoulou et al., 2023); on emigration issues (Akkaya & Krcmar, 2019; Beris et al., 2019; Tao et al., 2019; van Noordt & Misuraca, 2022); in the field of public finance and taxation (Akkaya & Krcmar, 2019; Aoki, 2020; Stamatis et al., 2020; Vassilakopoulou et al., 2023); in the postal services (Akkaya & Krcmar, 2019; van Noordt & Misuraca, 2022); in the administrative modernization agencies (Reis et al., 2020); in the education sector (Daniel et al., 2020); for passport requests and issuance (Antoniadis & Tambouris, 2021); in civil protection (Androutsopoulou et al., 2019); in the commercial registration (van Noordt & Misuraca, 2019); and in road safety concerns (Stamatis et al., 2020). While no studies on increasing awareness of computer crime were found in the public sector, there is interest in implementing conversational assistants in justice-related public services (Monteiro et al., 2022; Sivcevic et al., 2020).

At least ninety-nine positive attributes were identified that characterize chatbots in public domains (Q2), emphasizing their continuous operation (24 hr a day, seven days a week) (Androutsopoulou et al., 2019; Aoki, 2020; Hasal et al., 2021; Petriv et al., 2020; Reis et al., 2020; Rita & Shava, 2021; Sivcevic et al., 2020; Tambouris & Tarabanis, 2021; van Noordt & Misuraca, 2019; Vassilakopoulou et al., 2023). Diverse attributes such as speed (Vassilakopoulou et al., 2023), ease of use (Piccolo et al., 2021), free use (Piccolo et al., 2021), real-time support (Tao et al., 2019), and automated service (Cantador et al., 2021) are also addressed. In terms of usability, accessibility, and user experience, chatbots demonstrate high standards of accessibility (Sivcevic et al., 2020), focusing

on user satisfaction (Androutsopoulou et al., 2019; Cantador et al., 2021; Vassilakopoulou et al., 2023) and promoting their well-being (Piccolo et al., 2021), its inclusion (Tambouris & Tarabanis, 2021), and your mental health (Piccolo et al., 2021). Aspects were identified that could raise concerns related to AI (ethics, privacy, and security) (Susar & Aquaro, 2019) and the legal field (Akkaya & Krcmar, 2019), including data protection, responsibility, transparency, and clarity of the communication process).

The RQ3 reflects data related to the design or implementation of chatbots, regardless of whether it focuses on their suitability and relevance within an e-government context concerning computer crime awareness. In this context, there has been significant interest in aspects of computer crime involving children, such as sexual offenses (grooming or sexting) and cyberbullying. Regarding sexual offenses that may involve children, six solutions have been identified: the development of a website that offers awareness-raising materials and reporting tools for child victims of sexual crimes online. In this context, the possible implementation of chatbots on the platform is emphasized as a valuable asset for facilitating report submissions (Rita & Shava, 2021); the creation of a module for attracting sex preparers using an intelligent question-answer analysis engine, with a view to the automatic characterization of pedophile tendencies (Zambrano et al., 2017); the development of a model based on adolescent personality traits to detect pedophilic behavior on the Internet (Villatoro-Tello et al., 2016).; a system for detecting conversational patterns regarding child sexual predators across various internet platforms, including chat rooms, social networks, and other sites (Laorden et al., 2013); a module for interaction that acts as a decoy to identify potential sexual predators on various internet platforms (Murcia Triviño et al., 2019; Yoo & Cho, 2022); and a solution for identifying suitable dialogue flows for the potential design of a support chatbot aimed at children in online environments, considering issues like cyberbullying, grooming, and sexting through conversations between children and Lego figures (Piccolo et al., 2021). When considering computer security and cyberattacks, five solutions were identified: an antivirus module for detecting malware and phishing attacks using chatbots designed for integration with Messenger (Lee et al., 2020; Yoo & Cho, 2022).; a module to integrate WhatsApp for foundational concepts and security procedures for company employees, addressing emerging technologies and cyberattacks, while providing self-assessment and knowledge resources within organizations (El Hajal et al., 2021); selecting a suitable encryption method to protect vital information (Dan et al., 2019; Yoo & Cho, 2022) to implement a system for detecting the different stages of progress in a phishing attack, utilizing CNN classifiers and AI technology (Yoo & Cho, 2022); as well as corporate training in computer security (Kowalski et al., 2013; Yoo & Cho, 2022). In the context of RQ3, it is essential to note that the identified studies do not concentrate on the specificity or suitability of implementing chatbots in e-government or public administration platforms concerning computer crime awareness. Nevertheless, it is crucial to acknowledge the interest and relevance of using these conversational assistants to raise awareness about computer crime, particularly in a context where the safety of children and young people is a concern.

Regarding RQ4, no studies align with the predefined objectives of the research question about identifying studies aimed at implementing chatbots in an e-government context to raise awareness of computer crime. Nevertheless, four articles were identified that contain data, even if presented in an indicative manner, regarding the specific interest of public entities in the research topic. The Rita and Shava study (2021) focuses on creating a website featuring awareness materials and reporting tools for child victims of sexual crimes online. While the study suggests the potential integration of a chatbot, it does not address the context of e-government. Conducted in collaboration with the Namibian School System, the study notes that, while this solution could help address the issue, significant further action is needed involving additional organizations, including law enforcement agencies. The research conducted by Piccolo et al. (2021) aimed to identify suitable dialogue flows for the potential design of a support chatbot, in light of the increasing phenomena affecting children in internet environments, such as cyberbullying, grooming, and sexting, which may occur through conversations involving children and Lego figures. Furthermore, while this study does not address the specific context of e-government, it is noteworthy that the research received funding from the Open University's Centre for Policing Research and Learning and was supported by the Metropolitan Police. In Laorden et al. (2013), concerning the detection of conversational patterns of child sexual predators in pedophilia criminal phenomena on various internet platforms (chats, social networks, or other platforms), although no reference is made to the e-government context, mention is made of the fact that the Basque Government supported the research. In Yoo and Cho (2022), an article is referenced concerning a module that functions as a decoy to identify potential sexual predators on various internet platforms (Tambouris & Tarabanis, 2021). While the e-government context requires further examination, it is important to acknowledge the utility of the system for law enforcement agencies. Research related to RQ4 does not emphasize the importance and suitability of employing conversational assistants within e-government frameworks to enhance awareness of computer-related crimes. Moreover, it is essential to underscore the interest and support demonstrated by state agencies and public organizations, particularly law enforcement, in investigations concerning the application of chatbots to combat computer crime context.

In relation to RQ 5, the aspects of AI use focus on: the level of government policies (European Commission, 2021a; European Parliament & the Council of the European Union, 2018; Misuraca et al., 2020; Viscusi et al., 2020); their application by police and judicial authorities (European Parliament, 2021a; Leaua & Didu, 2021); their requirements and evaluation guidelines for implementation (European Commission, 2018; Hasal et al., 2021; Henman, 2020); their role as an instrument for modernizing PA (Gerontas, 2020); and intellectual property rights (Leaua & Didu, 2021; The European Parliament, 2020). Regarding interoperability in the public sector (European Commission, 2010; 2017) it is a

critical success factor for increasing efficiency, transparency, quality, and cooperation in PA (Antoniadis & Tambouris, 2021; Gerontas, 2020; Tambouris & Tarabanis, 2021). Concerning data protection and security (European Parliament & the Council of the European Union, 2016; International Organization for Standardization, 2005) the rules of the *General Data Protection Regulation (GDPR)* regarding the processing and transfer of personal data (Akkaya & Krcmar, 2019; Carvalho et al., 2020; Hasal et al., 2021; Viscusi et al., 2020) were identified. The ethics field (European Parliament, 2021b) refers to the European Union's recommendations on the legal regime concerning the various ethical aspects of AI, robotics, and related technologies (Leaua & Didu, 2021; Susar & Aquaro, 2019). The strategies for promoting digital skills refer to the program *National Digital Skills Initiative e.2030 - INCoDe.2030* (Presidency of the Council of Ministers, 2018), which aims to implement measures to increase personal skills in the new digital technologies (Reis et al., 2020). On cybersecurity strategies at the European level (European Commission, 2020b), resilience, technological sovereignty, and leadership are mentioned to prevent and respond to cyberspace incidents. The importance of developing global cyberspace with reinforced international cooperation is also discussed (Carvalho et al., 2020; Ubowska & Królikowski, 2022). The report *Architecture for Public Service Chatbots* (European Commission, 2019a) aims to guide the appropriate design of architectures, including the conception and development of chatbots in public services.

Concerning RQ6, the main factors identified involve digital accessibility issues, including the information and communication technology requirements for people with disabilities (European Commission, 2021b; Gaggi & Perinello, 2022); enhancing the accessibility of public sector websites and mobile applications (European Parliament & of the council, 2016; Gaggi & Perinello, 2022); and establishing guidelines for creating more accessible web content for individuals with disabilities (Gaggi & Perinello, 2022), addressing visual, auditory, physical, speech, cognitive, linguistic, learning, and neurological aspects (Web Accessibility Initiative Group, 2023).

In conclusion, this systematic literature review highlights the significance of the research topic, emphasizing the necessity for further exploration in this important domain of knowledge potential.

2.4.2. Scoping review

Considering the study's specific objectives related to exploring and mapping evidence on a particular topic, this review was drafted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews (PRISMA-ScR) (Tricco et al., 2018). This scoping review identified important factors for designing and evaluating chatbot architectures in public administration, aligning with the stated objectives. The review aims to thoroughly assess elements that can impact chatbot development and evaluation in this sector. By analyzing key features, we seek to uncover research gaps and improve the design and evaluation processes, ultimately enhancing chatbot effectiveness, especially in the justice domain of the public sector.

In our search strategy, we established criteria for selecting studies to ensure they align with our research scope and focus on essential public administration or e-government objectives. From the beginning, we excluded any articles that did not meet these criteria. The studies needed to have undergone peer-review processes and be published between 2018 and 2023. Over a two-week period in April 2023, we searched for and reviewed titles, abstracts, and full texts of studies from the ACM Digital Library, IEEE Digital Library, ISI Web of Science, ScienceDirect, Scopus, and Wiley Online Library databases. We conducted an extensive search using a variety of terms and their synonyms related to chatbots (virtual assistant and conversational assistant), public administration (e-government, electronic government, and digital governance), development (software, tools, frameworks, design, technology, and methodology), and evaluation (testing, performance, metrics, validation, and assessment). We created a data extraction form that included the items described in each of the 22 selected studies in this review. The extracted data was synthesized using a narrative approach.

The SR identified the concepts that characterize and interfere with the development of chatbots (RQ1), the principal methodologies guiding their development (RQ2), the technologies influencing their development (RQ3), the architectures suitable for their development (RQ4), the relevant tools for their development (RQ5), and the principal methods for their evaluation (RQ6)

Regarding Q1, there is significant interest in interoperability among public services, particularly in concepts that can foster the development of chatbots related to the electronic cooperation of organizations (Gerontas, 2020), the provision of shared services (Reis & Melao, 2023), the availability of tools for evaluating and optimizing resources (Gerontas, 2020), and solutions that can integrate ethical factors (Bang et al., 2021).

Regarding research methodologies (Q2), the *Design Science Methodology* (Hevner et al., 2004; Peffers et al., 2007), and the *Chatbot Management Process Methodology* (de Andrade et al., 2020) were identified. Public service models can use DSR concepts to explore how humans create artifacts to achieve measurable goals (Hevner & Storey, 2023).

Considering technologies that can influence the implementation of chatbots in the public sector (Q3), several factors identified are related to: AI-enabled chatbots in the NLG, NLP, and NLU domains (Antoniadis & Tambouris, 2022; Hasan et al., 2021); the implementation of high scalability rates (Wilson & Marasoiu, 2022); predefined conversational flows in the context of close-domain chatbot development (Hasan et al., 2021; Mahmoud & Kumar, 2020); the choice of models based on deterministic rules, to the detriment of probabilistic models (Santos et al., 2022); and the avoidance of generative models, which are inherently unclear and utilize external datasets (Bang et al., 2021). It is also essential to consider models that place a strong emphasis on ethical issues regarding data and conversational flows (Daniel et al., 2020), as AI involves factors such as

transparency, predictability, accountability, fairness, privacy, and control (Bang et al., 2021).

In architecture models (Q4), there are several attributes to consider: the use of cloud-based computing resources, which effectively cover the entire architecture and components of the solution (do Rosário Valverde & Couto e Vasconcelos, 2019); the importance of ethics-related issues (Bang et al., 2021); the integration of solutions utilizing open source resources (de Lacerda & Aguiar, 2019); the significance of governance factors (Hevner & Storey, 2023), including user feedback (do Rosário Valverde & Couto e Vasconcelos, 2019); the interest in employing machine learning (Mahmoud & Kumar, 2020); and the emphasis placed on the Core Public Service Vocabulary (CPVS models) (Antoniadis & Tambouris, 2022; do Rosário Valverde & Couto e Vasconcelos, 2019), particularly regarding resource sharing among public entities. Additionally, the information and services provided by the conversational assistant should also be accessible from the internet portal where it is implemented (do Rosário Valverde & Couto e Vasconcelos, 2019).

Despite the availability of many tools for chatbot development (Q5), it is crucial to consider the European guidelines in the *Architecture for Public Service Chatbots* report (European Commission, 2019a). This report emphasizes cloud computing services in a SaaS context paradigm. These platforms provide high levels of stability, scalability, and resource resilience, ensure the security and audibility of their architectures, and enable chatbots to be replicated via API across various PA bodies (European Commission, 2019a). Solutions capable of meeting these requirements were mentioned (European Commission, 2019a), including Dialogflow (Google), Watson Assistant (IBM), Amazon Lex (AWS), and Azure Cognitive Language Services (Microsoft). These resources greatly enhance accessibility, personalization, community support, cost efficiency, transparency, security, and education (Antoniadis & Tambouris, 2022; de Lacerda & Aguiar, 2019).

Various methods for chatbot evaluation were identified (Q6), including web platforms like ChatEval (Sedoc et al., 2019) and various metrics based on Nielsen's 12 heuristics (de Lacerda & Aguiar, 2019; Höhn & Bongard-Blanchy, 2021), which rely on users' subjective perceptions. The Chatbot Performance Evaluation (Nirala et al., 2022) encompasses processes concerning scalability factors, the application of the Turing test, the significance of interoperability elements, efficiency, and the speed of query-response interactions. The Technology Acceptance Model (TAM) (Davis, 1993) assesses perceived usefulness, ease of use, user attitudes toward the chatbot, and behavioral intentions for continued use (Antoniadis & Tambouris, 2022). The System Usability Scale (SUS) (Bangor et al., 2008; Usability.gov, n.d) is mentioned in relation to usability. One notable aspect of this solution is its validation in the Portuguese context (Martins et al., 2015).

3. Research approach and methodology

The primary objectives of the research were to conceptualize, develop, and validate a chatbot for integrating public administration websites and increasing awareness of computer crime. The study follows Peffers et al.'s Design Science Research (DSR) methodology (Peffers et al., 2007).

This research method has been widely adopted in information systems and is crucial for addressing complex problems (Hevner et al., 2004). Given the objectives focused on developing an artifact (chatbot), the DSR methodology (Hevner et al., 2004) provides a solution with a robust theoretical foundation to support the development and scientific validation of the work. According to Peffers et al. (Peffers et al., 2007), DSR consists of six stages (Figure 1): problem identification and motivation, definition of the solution's objectives, design and development, demonstration, evaluation, and communication.

Step 1 - Problem Identification and Motivation. During this phase, the research problem was clearly defined and justified, accompanied by an artifact designed to address it (Peffers et al., 2007). The focus is on identifying the best methods to raise public awareness about computer crime. This phase, which heavily relied on documentary research, aimed to establish the significance of the issue, highlight the necessity for solutions, and investigate possible strategies. It pinpoints the right technological tools and suitable implementation environments needed for effective, credible, and comprehensive promotion of awareness concerning computer crime way.

Step 2 - Defining a Solution's Objectives. After establishing the problem's significance and showcasing its relevance, we can outline the solution's objectives. The goal is to examine previously implemented solutions, whether in whole or in part (Peffers et al., 2007), through documentary research processes and the initial phase of the literature review, by referencing a systematic literature review.

Stage 3 - Design and Development. In this phase, creating the artifact determines the desired functionalities and corresponding architecture, culminating in prototype design. The resources needed for this phase include applying theoretical knowledge from a particular solution (Peffers et al., 2007). By utilizing documentary research processes within the framework of the second phase of the literature review, which involves a scoping review, the aim was to identify, within an e-government context, the concepts that can influence the development and evaluation of chatbots.

Step 4 - Demonstration. At this stage, it was essential to assess whether the artifact's use, in whole or in part, addresses the defined problem. It includes the necessary knowledge to utilize the artifact in resolving the issue. It encompasses the potential for the artifact to fulfill its intended role (Peffers et al., 2007). By the end of this phase, the goal was to provide a functional artifact emerging from the development stage, equipped with characteristics suitable for integration into PA websites to raise awareness about computer crime. This activity resulted in iterations of the previous phases for implementing improvements.

Stage 5 - Evaluation. The evaluation phase focuses on assessing how effectively the artifact addresses the identified problem. The goals outlined in the solution are compared against the results generated from using the developed

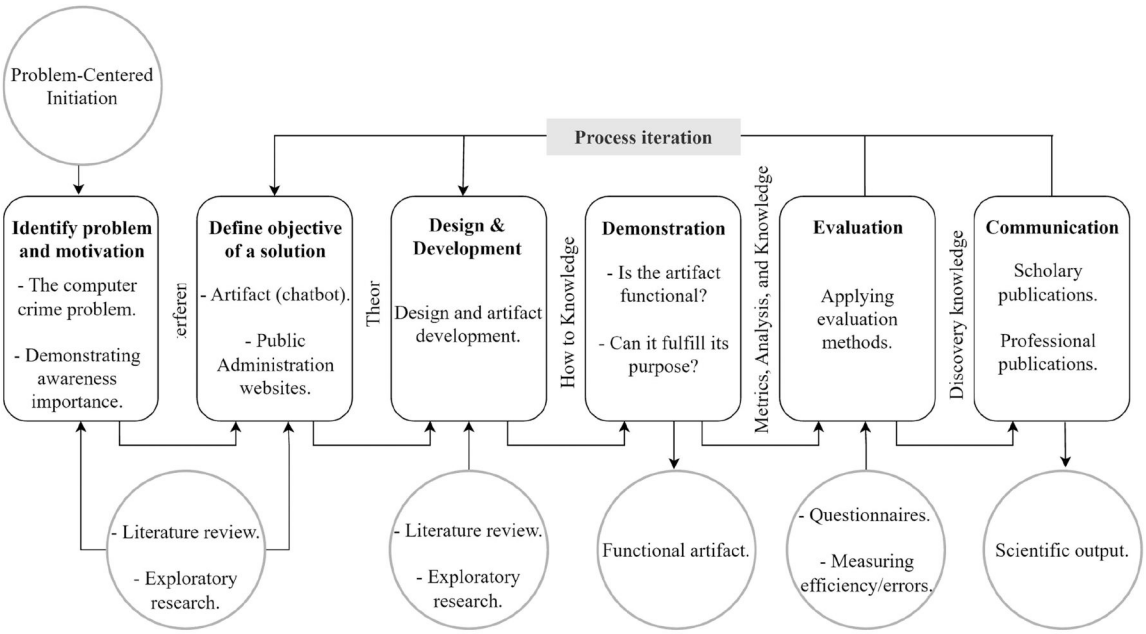

Figure 1. Design science research (DSR). Adapted from peffers et al. (Peffers et al., 2007).

artifact (Peffers et al., 2007). Electronic questionnaires facilitate data collection and analysis, allowing for an evaluation of the artifact across various dimensions, particularly its efficiency and intended purpose (Creswell & Creswell, 2018; Jain et al., 2018; Peras, 2018). The System Usability Scale (SUS) usability test was conducted (Bangor et al., 2008; Usability.gov, n.d), considering the details mentioned in (Martins et al., 2015). Furthermore, it examined the data from user interactions with the artifact, collected through analytical tools on the chatbot's implementation platform, to assess the effectiveness of conversational flows and analyze failures in understanding intentions and entities. This process led to revisions of the earlier phases for implementation improvements.

Stage 6 - Communication. The communication process related to this undertaking encompasses scientific and professional journals, emphasizing utility, functionality, innovation, scientific rigor, and the breadth of the results obtained (Peffers et al., 2007).

4. Design and prototype development phase

The design and development phase of the artifact was based on the literature review and documentary research. Multiple research projects were conducted on various functional requirements and available resources from chatbot development platforms that had no financial charges and aligned with the investigated parameters and purposes. Initially, the features offered by Google (Dialogflow), Microsoft (Azure), and IBM Cloud (Watson Assistant) were explored and tested. One limitation identified during the functional testing of these platforms was the deficiency of resources accessible in the evaluation accounts, particularly concerning time constraints. Given that Watson Assistant did not impose such time limitations, this became a significant factor influencing a more comprehensive understanding of its diverse capabilities. The principal investigator's profound expertise with the Watson Assistant platform, coupled with the supplementary time allocated for a more thorough comprehension of the other platforms, ultimately reinforced this understanding choice.

4.1. Requirements for chatbot development

User and artifact operation requirements were established during the computer system or application development process (Corea et al., 2020). User requirements refer to users' expectations and needs, expressed in abstract terms, without necessarily being concerned with the technical implementation of the solution. These expectations encompass the interface's ease of use, the system's expected performance, the capacity for customization, and other acceptance criteria (Corea et al., 2020). Functional requirements describe the system's functionality in both form and operation, expressed through use cases, system requirements, and detailed specifications of various functionalities. They should include the functions or services the system provides to satisfy user requirements (Corea et al., 2020). The artifact's architecture was based on the technical guidelines of the Watson Assistant platform regarding functional requirements, along with the theoretical aspects already covered. The user requirements related to the expectations and objectives of the artifact's implementation, which is associated with raising awareness of computer crime, were defined in the evaluation phase.

4.2. Description of architecture components

Technically, chatbots generally consist of three essential elements: the interface, the natural language processing (NLP) engine, and the knowledge base. The interface can take different forms, such as a website, instant messaging, or a

mobile app. The natural language processing engine manages the semantic context of conversations. In turn, the knowledge base serves as the central core of content that enables interactions (Nirala et al., 2022). Considering the knowledge base, there are three main types of chatbots: rule-based, retrieval-based, and generative (generative-based) (Adamopoulou & Moussiades, 2020). Rule-based chatbots operate according to a fixed set of guidelines (decision tree models) for user interaction. These chatbots provide predefined responses to users' questions and do not learn from these interactions. Retrieval-based chatbots also deliver predefined answers but utilize some heuristics to extract answers, creating shortcuts compared to the entire decision tree method. Although they may include elements of AI, these chatbots cannot generate completely new responses (Manzoor & Jannach, 2021). Using generative methods, such as OpenAI ChatGPT (OpenAI, n.d), Chatbots can create dialogues using large volumes of conversational data. The model based on generative methods can utilize a combination of techniques, including supervised and unsupervised learning, reinforcement learning, and adversarial learning (Androutsopoulou et al., 2019). Chatbots can engage in brief conversations to provide a singular answer to questions in a Q & A format, while longer discussions permit the exchange of substantial amounts of information throughout a conversation (do Rosário Valverde & Couto e Vasconcelos, 2019). Despite the many advantages and potential of implementing chatbots in the public sector, certain attributes, such as generative models, may require attention. In this context, various discussions about ethical considerations, security, and user privacy related to artificial intelligence (AI) topics (Susar & Aquaro, 2019) are related. There are also legal issues at stake, including data protection (Akkaya & Krcmar, 2019), the accountability and transparency of the information presented in conversational flows (Akkaya & Krcmar, 2019), and the form and clarity of communication processes (de Melo & Monteiro, 2021).

The large number of users and the high traffic generated by PA raise the importance of solutions based on cloud computing services (European Commission, 2019a). Guidelines for chatbot architectures in public services (European Commission, 2019a) and the literature review also emphasize the importance of cloud computing platforms (European Commission, 2019b). Watson Assistant, from IBM Cloud, offers various ways of integrating chatbots into websites with high-security standards, authentication mechanisms, and scalable resources (IBM, n.d.b; IBM, n.d.a). This platform has features suitable for research, such as AI in the advanced NLP resources and machine learning capabilities (IBM, n.d.b; IBM, n.d.a). Watson Assistant provides advanced natural language capabilities, with a combination of natural language understanding (NLU), natural language processing (NLP), and natural language generation (NLG) capabilities (IBM, n.d.b). The API resources provided by Watson Assistant offer the functionalities suggested in the literature review in a scalable format (IBM Cloud - Watsonx Assistant, n.d). The *Discovery* tool (IBM Cloud - Watson Discovery, n.d) increases natural language processes, extending the search for possible answers to different types of documents that can be integrated into the knowledge base. The *Language Translator* tool can implement multilingual resources, while the *Tone Analyzer* tool can improve feedback processes (IBM, n.d.b; IBM, n.d.a).

Regarding ethical considerations, Watson Assistant incorporates features that directly address ethical, legal, and technical concerns related to using chatbots for computer crime awareness, including data protection (Akkaya & Krcmar, 2019), mitigation of algorithmic biases, and combating disinformation (Susar & Aquaro, 2019). Its architecture, based on deterministic models, predefined rules, and knowledge retrieval (Adamopoulou & Moussiades, 2020), offers predictability, transparency, and auditability of responses- qualities deemed essential for the institutional credibility of public entities (European Commission, 2018; European Parliament, 2021a). Additionally, Watson Assistant provides robust mechanisms to ensure compliance with regulations like GDPR, utilizing advanced data control, anonymization, consent management, and interaction encryption (Akkaya & Krcmar, 2019). These characteristics contrast with the limitations of generative models, which, despite their creative capacity and dynamic interaction (European Commission, 2019a), are less suitable for the public administration environment due to their complexity, risks of inaccurate responses, and challenges in auditing (European Commission, 2019a; Manzoor & Jannach, 2021). In this context, utilizing rule-based chatbots or knowledge retrieval is more appropriate, as it ensures clarity in communication processes (de Melo & Monteiro, 2021), accountability, and standardization of responses among various public entities (European Commission, 2013), while also respecting intellectual property (Leaua & Didu, 2021; The European Parliament, 2020).

Watson Assistant also stands out due to its integration with complementary tools, such as Watson Discovery (IBM Cloud - Watson Discovery, n.d), which broadens the search for answers in structured knowledge bases; Language Translator, which facilitates the creation of multilingual chatbots (IBM, n.d.b; IBM, n.d.a); and Tone Analyzer, which tailors responses based on the user's emotional context, fostering ethical and effective communication (IBM, n.d.b; IBM, n.d.a). By aligning with best practices recommended in the literature—including predictability, transparency, security, and data governance (Akkaya & Krcmar, 2019; Susar & Aquaro, 2019)—and adopting deterministic and auditable architectures (Adamopoulou & Moussiades, 2020), Watson Assistant establishes itself as a scalable and dependable solution for implementing public chatbots, addressing the ethical, legal, and technological challenges inherent to applied artificial intelligence.

In the specific domain of security components, particularly regarding the protection of the Watson Assistant structure and the accuracy of the knowledge base contents, IBM Cloud (IBM, n.d.a) states that security issues encompass multiple dimensions. These include the security and encryption of data transferred to its services- whether from customer data centers or other cloud-based services- verifying user identities and access rights to information along with the platform's AI features and ensuring secure access to the

API services available on its platform and in customers' data centers. IBM Cloud's security concerns involve the encryption and protection of generated data. Key factors include verifying user identities on the platform, controlling access to AI features, and securing APIs (IBM, n.d.b; IBM, n.d.a). IBM Cloud (IBM, n.d.a) provides security and authentication features for accessing personal accounts, including Multi-Factor Authentication (MFA) and Identity and Access Management (IAM). It also supports the external sharing of APIs through Service IDs and their respective authentication keys. These features are designed with the user in mind, ensuring a user-centric approach to security. In addition to these features, other services offered by IBM Cloud include IBM Security QRadar SIEM, IBM Cloud Security, IBM Security Access Manager, IBM Activity Tracker, IBM DataPower Gateway, IBM Cloud Data Encryption Services, IBM Key Protect, and IBM Security Directory Suite. Watson Assistant enables the monitoring, analysis, and optimization of chatbot performance through the *Analytics* tool (IBM, n.d.a; IBM Cloud - Watsonx Assistant, n.d). This allows error detection, identification of popular topics, optimization of the effectiveness of responses, sentiment analysis, feedback analysis, and decision-making for strategic planning and continuous improvement processes.

4.3. Artefact integration concepts

Factors such as transformation and digital connectivity in PA (Ubaldi et al., 2019) are crucial to modernizing services, improving their efficiency, and ensuring that the State can effectively meet the needs of its citizens (Filipe et al., 2012). These efforts create responsive, transparent, citizen-centered governance structures (European Commission, 2016). We can see the importance of emerging technologies in the public sector, such as AI (Henman, 2020; Ubaldi et al., 2019) when applied in chatbots (Kumar & Mukund, 2020; Zuiderwijk et al., 2021). Public administration services should consider citizens' active participation in digital resources (Tavanapour et al., 2020), providing recommendations for organizing and integrating digital resources (European Commission, 2020a). They must also consider feedback factors related to analyzing reactions through automatic learning or direct monitoring of conversations (European Commission, 2019a). The PA must make intelligent digital communication channels available, including automated assistance (Maragno et al., 2023). When multilingual resources are introduced, the quality and quantity of communication processes increase (Tambouris & Tarabanis, 2021). PA websites must be accessible to all users, including people with disabilities (European Parliament & of the council, 2016). Accessibility attributes (Sivcevic et al., 2020), usability, and user experience (Androutsopoulou et al., 2019; Cantador et al., 2021; Vassilakopoulou et al., 2023) should be considered to promote their well-being (Piccolo et al., 2021). The Watson Assistant platform can use *Speech-to-Text*, *Text-to-Speech*, and *Language Translator* resources to increase this paradigm. Interoperability between public sector entities (European Commission, 2010; 2017) refers to the continuous exchange of information between the different systems and platforms of various services and is seen as a critical success factor for increasing efficiency, transparency, quality, and cooperation in PA (Antoniadis & Tambouris, 2021; Gerontas, 2020; Tambouris & Tarabanis, 2021). Chatbots boost organizations' electronic collaboration by providing tools for evaluating and optimizing resources (Gerontas, 2020). Chatbots' credible content is essential to public entities' institutional image (European Parliament, 2021a, 101). Therefore, it is critical to address issues of AI in the areas of ethics (Susar & Aquaro, 2019), accountability, and transparency of conversational flows (Akkaya & Krcmar, 2019), as well as the form and clarity of these communication processes (de Melo & Monteiro, 2021). It is essential to standardize content between PA entities (European Commission, 2013) and respect intellectual property rights when designing technologies that use AI (Leaua & Didu, 2021; The European Parliament, 2020). Chatbots must provide relevant information in the initial interface related to a description of their purpose and the terms of the services. Other factors are related to the purpose of the chatbot, the preservation and protection of personal data, the possibility of not using the service, the provision of alternative contact channels, and the circumstances relating to privacy and security issues (European Commission, 2019a). It is becoming critical for the PA to make websites and mobile applications more accessible to users (European Parliament & of the council, 2016). Given the growing use of use smartphones, it is essential to optimize the experience of using chatbots through mobile devices (European Commission, 2019a). In addition to the communication channels that the chatbots constitute, the PA should provide other forms of communication, either through a human agent (email or telephone) or by directing users to other specialized chatbots (European Commission, 2019a).

4.4. Logic chatbot architecture proposal

Figure 2 incorporates the guidelines and paradigms for the artifact architecture design into the description of components and concepts of the chatbot architecture proposal. In the context of e-governance policies (3), the digital transformation and connectivity processes (2) from PA (1) enable the implementation of intelligent communication channels (4). These intelligent communication channels (4) adopt automated assistance technologies, such as chatbots (5), which can play an essential role in communication strategies in mass actions to raise awareness of computer crime (7). The awareness content (8), adopted in the paradigm of interoperability between PA services (6), must be characterized as professional (9), credible (10), and endowed with ethical principles (12). The interoperability paradigm (6) also extends to sharing resources resulting from a single digital communication channel (4, 5) between the various PA websites (12), thus leading to the replication of the same chatbot (5, 13). The digital resources made available by the PA, mainly through its websites (12) and integrated chatbots (5,13,14), have characteristics suitable for use on multiple platforms (19) and electronic devices (20), particularly mobile devices (21), with respect for high standards of user

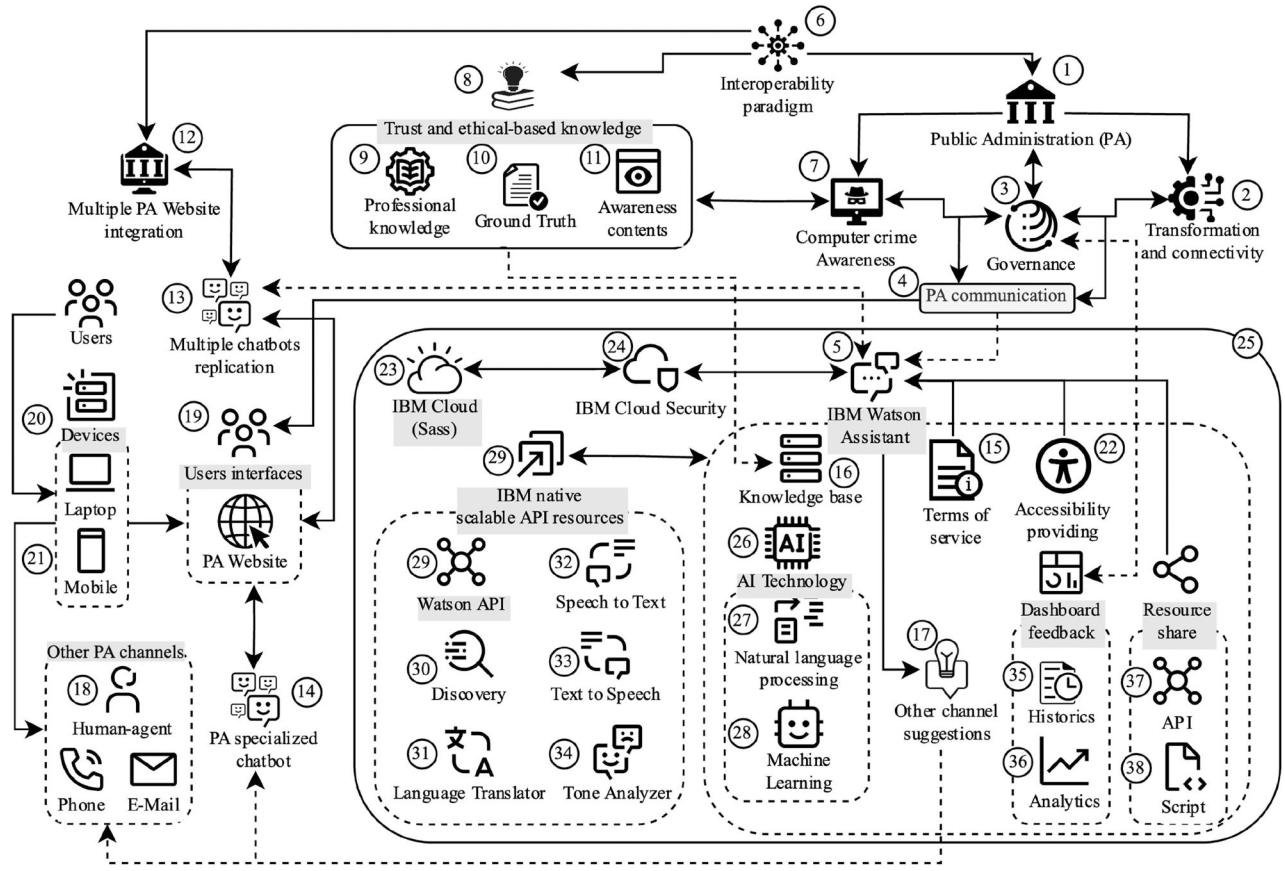

Figure 2. Proposed artifact architecture model.

experience, in aspects such as accessibility and usability (22). When conversational assistants integrate advanced cloud computing solutions on a software-as-a-service basis, they can improve the efficiency of their development, implementation, management, and use processes (23). The IBM Cloud (23), through Watson Assistant (5), secures (24) a wide range of resources and technologies that enable the development, implementation, and management of intelligent chatbots. These frameworks incorporate all the appropriate tools and technologies for the intended purpose into a single computing infrastructure (25). Watson Assistant (5) and IBM Cloud (23) natively make various tools and services via API (29) available in a scalable way, including *Watson Discovery* (30), *Language Translator* (31), *Speech-to-Text* (32), *Text-to-Speech* (33), and *Ton Analyzer* (34).

4.5. Main vectors of architecture design artifact

The main guidelines and components of the artifact took into consideration, in addition to the literature review, the theoretical and practical design concepts made available by Watson Assistant (IBM, n.d.a; IBM Cloud - Watson Assistant, n.d.a), reflected in the architecture described in Figure 2, the theoretical and practical design concepts made available by Watson Assistant. In the planning phase, the knowledge area's specific needs and the conversational assistant's characteristics were considered (IBM Cloud - Watson Assistant, n.d.a). Figure 3 describes the tasks required in the planning process to idealize a chatbot's basic architecture (IBM, n.d.a; IBM Cloud - Watson Assistant, n.d.a). The following factors were considered: definition of goals, objectives, and implementation channels (1); identification of intentions (2); the definition of entities (3); cataloging of the content collected in training, validation and test sets (4,5,6,7); identification and modeling of conversational flows and their context attributes (8); mapping the execution of intentions to existing process flows (9); identification of content sources, whether through shared repositories, public sources, multimedia content (6).

As described in Figure 4, the preparation and implementation phase involved the knowledge structure and the IT platform tools in the training, testing, and configuration processes.

This phase involved preparing the entities' content sources as part of their governance operations, related to: the creation of the chatbot (3); the creation and association of the dialog skill (4); the creation of the intents and intent utterance (5); the creation of the entities (6); testing the system (7); structuring the conversational dialogs flows (8); testing and intermediate evaluation of the model's performance (9); testing and intermediate assessment of the dialog flow (10); implementing and monitoring the model (11,12); and continuous processes of machine learning and adaptation.

Figure 5 shows the process of executing the basic architecture of a chatbot. In addition to the digital transformation and connectivity paradigms, the component refers to: conversation connection points located in the entities'

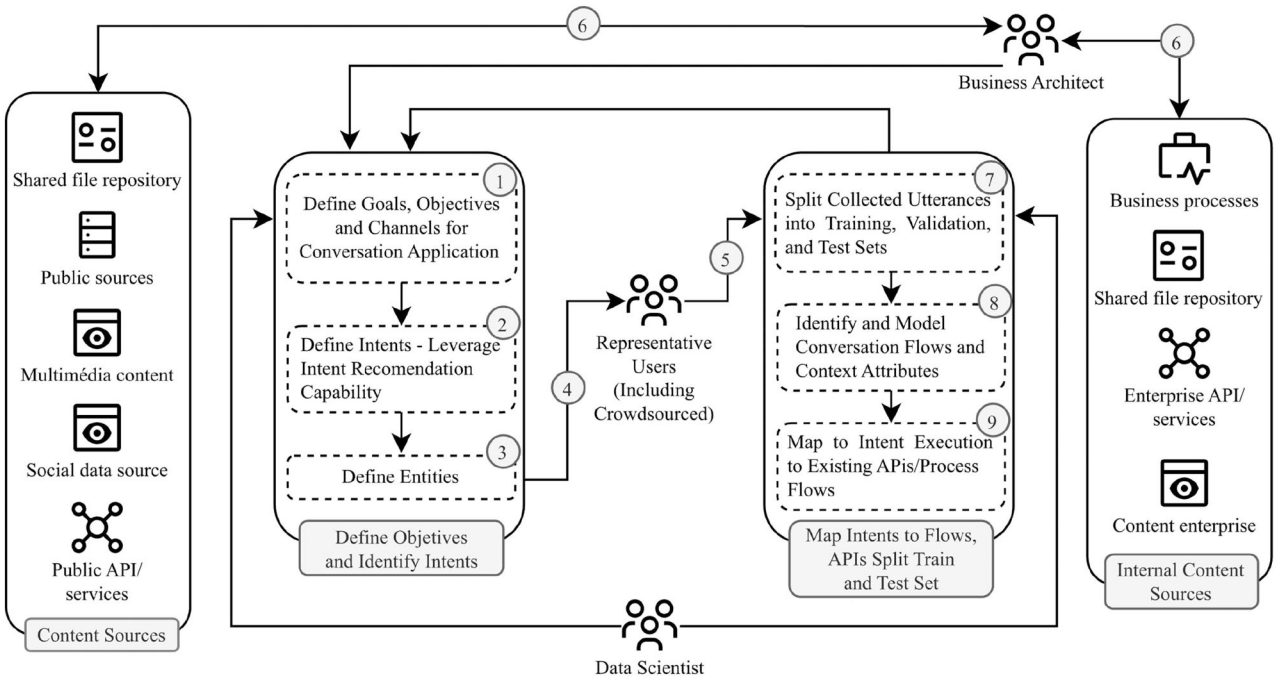

Figure 3. Planning phase proposed by watson assistant. Adapted from (IBM, n.d.a).

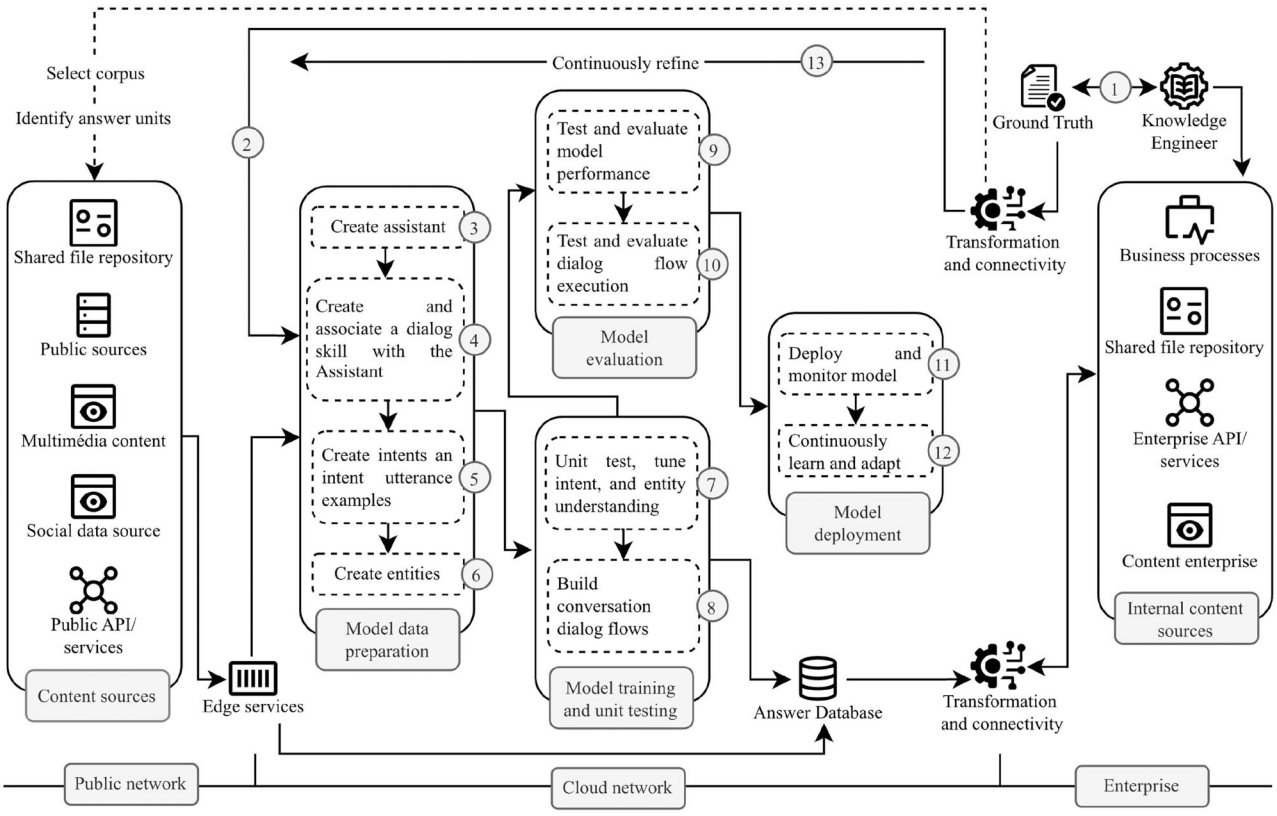

Figure 4. Preparation and implementation phase proposed by watson assistant. Adapted from (IBM, n.d.a).

network (1); conversation connection points located in the public network (2); and guarantee of truth and reliability associated with the entities' institutional governance (3); implementation and training components (4); *IBM Discovery* tool (5); knowledge base and responses (6); the process of interaction between user and conversational assistant, using electronic devices (7); IBM *Speech-to-Text* tool (when integrated) (8); computer application logic and structure (9).

The knowledge base and the dialogue flows for the chatbot on computer crime awareness (Appendix 1, supplementary material) were developed using trusted sources from

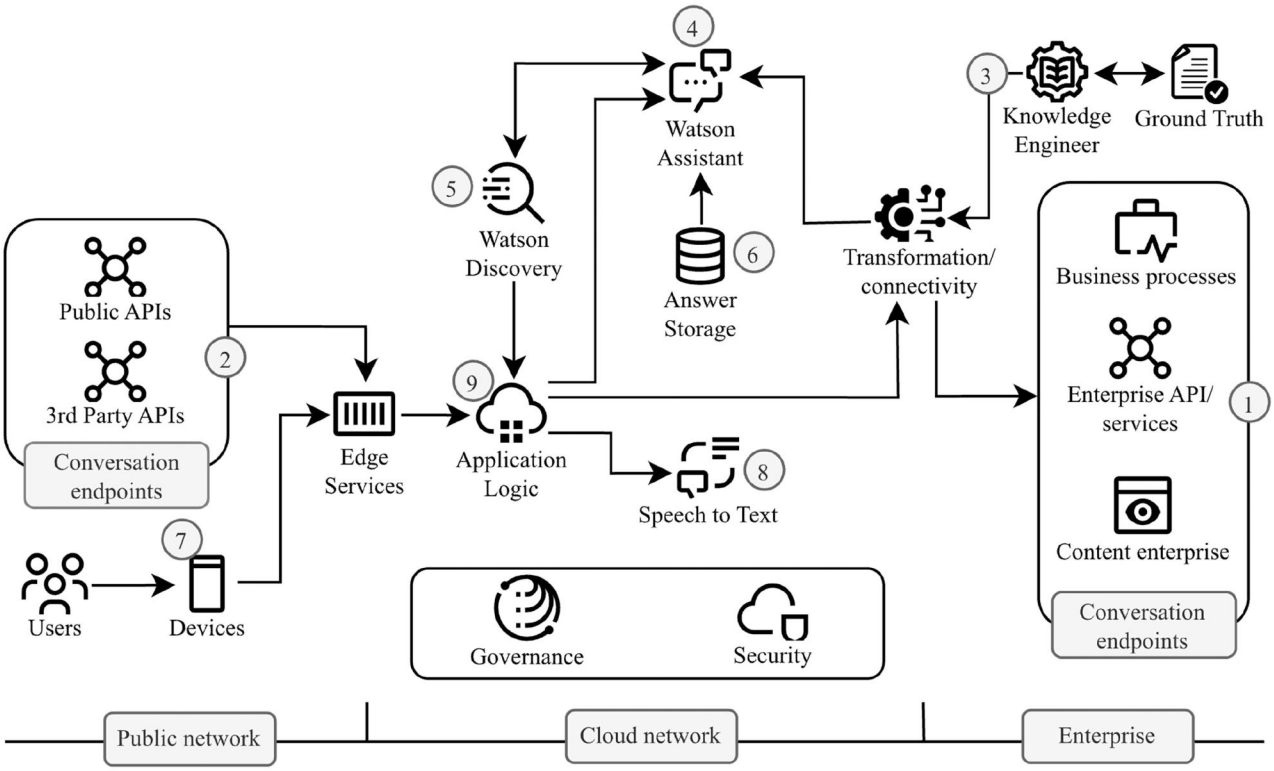

Figure 5. Execution process of the architecture proposed by watson assistant. Adapted from (IBM, n.d.a).

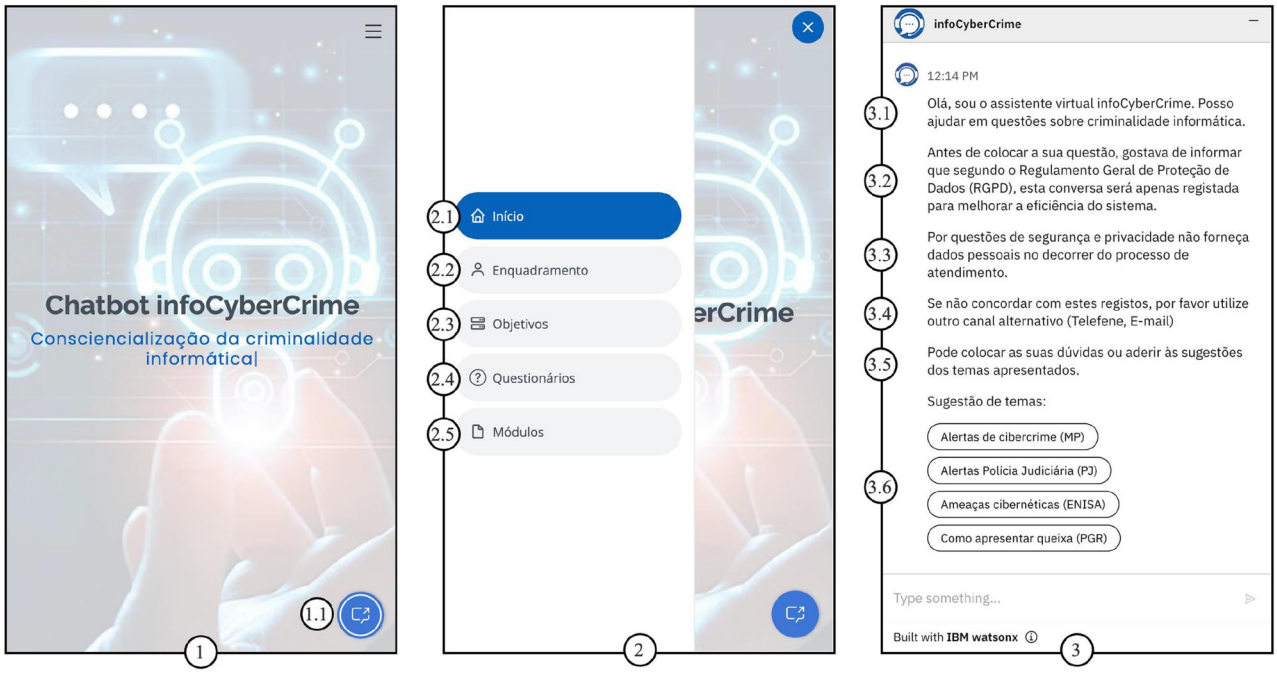

Figure 6. Website modules integrating the artifact (chatbot) (Pimentel, n.d).

Portugal and European entities, ensuring its ethical and trustworthy nature.

5. Prototype demonstration phase

In this phase, the aim was to demonstrate the efficiency of the conversational flows through random operation and performance tests and the reliability of the chatbot information.

As described in Figure 6, a website was implemented on the *Cloud Object Storage* (IBM Cloud) (IBM, n.d.a) (1,2,3) to carry out the practical aspects of the demonstration and evaluation phases. The chatbot was integrated through the API (Java Script) (IBM Cloud, n.d.a) available from Watson Assistant (IBM Cloud, n.d.b). Multifactor authentication was implemented to access the IBM Cloud account, while API integration was carried out using the Service IDs and authentication keys.

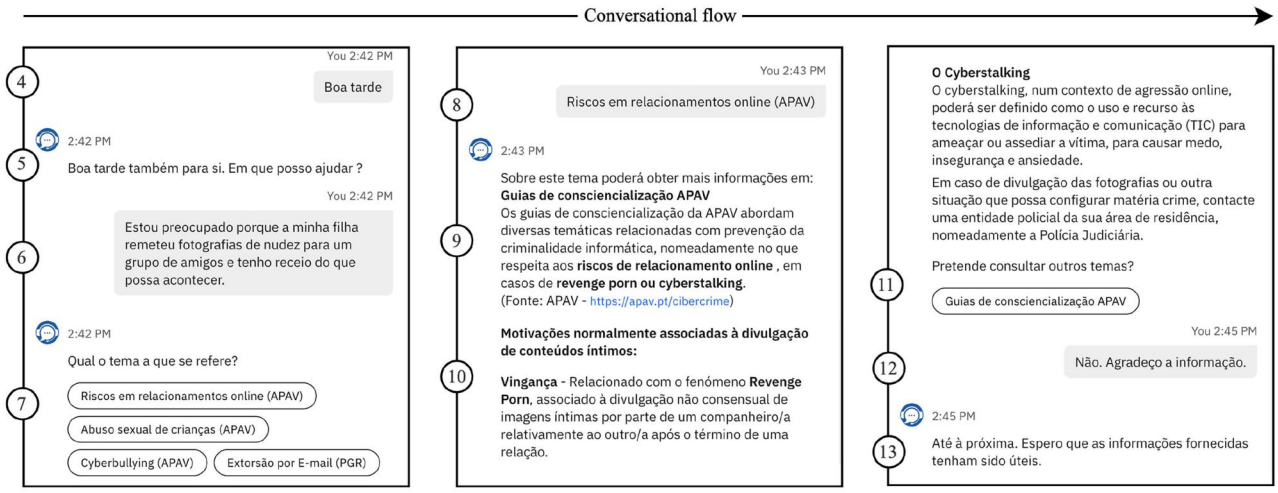

Figure 7. First use case (demonstration phase).

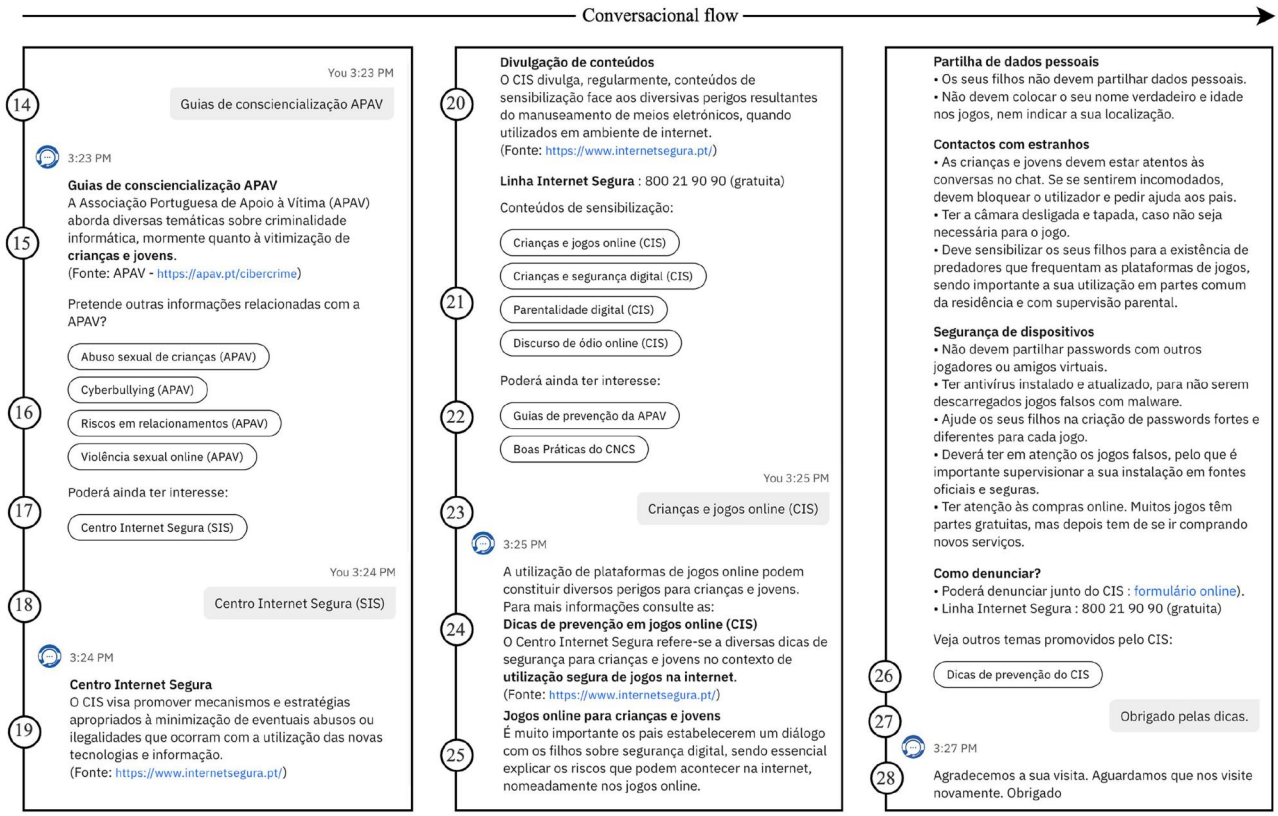

Figure 8. Second use case (demonstration phase).

In this phase, the aim was to demonstrate the efficiency of the conversational flows through random operation and performance tests and the reliability of the chatbot information.

In the first use case (Figure 7), after was asked: "*I am worried because my daughter has sent nude photos to a group of friends, and I am afraid of what might happen*" (6), the chatbot suggestions were related to the risks of online relationships, child sexual abuse, cyberbullying, and extortion by email (7). Given the response to the dangers of online relationships, more information was obtained (8). The chatbot shared information about the motivations that led to the illicit disclosure of intimate content involving young people, in terms of revenge porn and cyberstalking, as well as the possibility of filing a criminal complaint about what happened (10).

In the second use case (Figure 8), after being asked about children and online games (8), the chatbot provided information about the awareness-raising content (25) associated with maintaining a dialog with children and young people, care when sharing personal data, the dangers of contact with strangers, the security of electronic devices, and reporting forms (25).

In the third use case (Figure 9), after the chatbot was asked, "*What are the most recent alerts for computer crime*

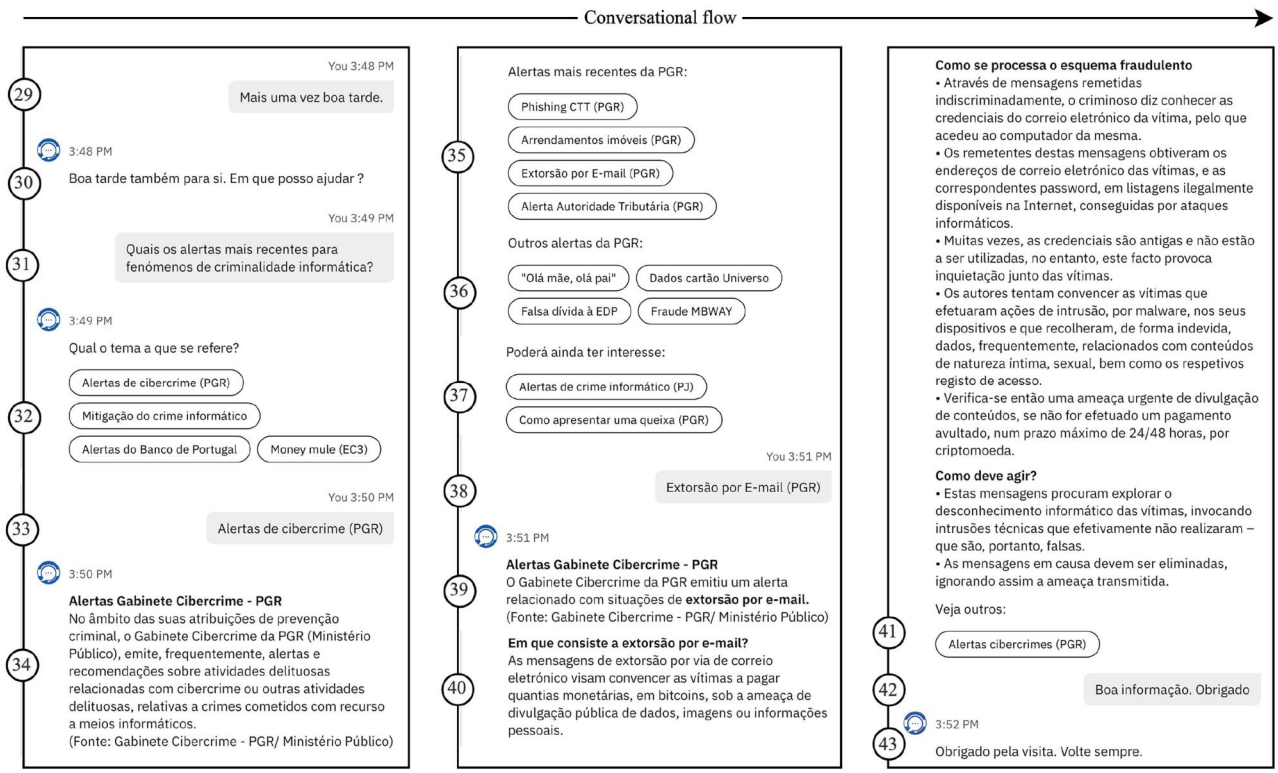

Figure 9. Third use case (demonstration phase).

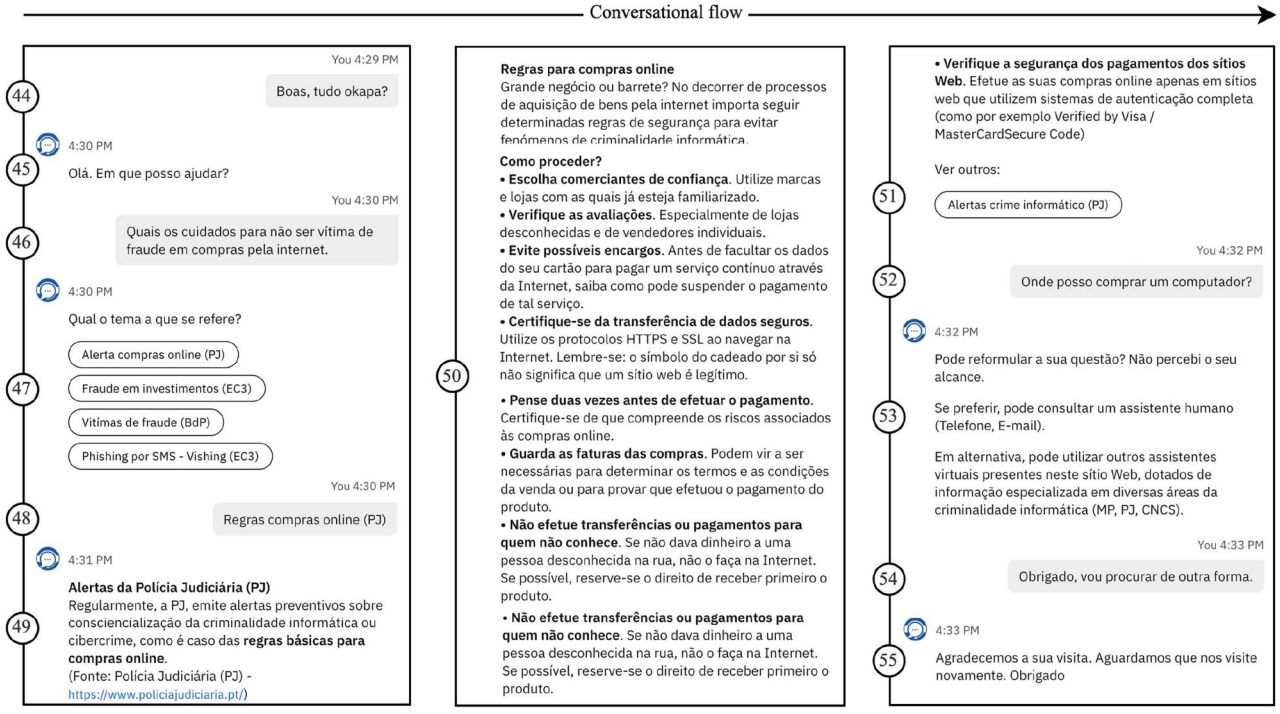

Figure 10. Fourth use case (demonstration phase).

phenomena?" (31), contextualized the request regarding possible intentions (32) related to cybercrime alerts, the mitigation of computer crime, financial alerts, and the money mule criminal phenomenon. After we opted for the suggestion of email extortion, the chatbot summarized the phenomenon, describing how the process unfolds and forms of prevention (40).

In the fourth use case (Figure 10), after being asked about "*How to avoid becoming a victim of internet shopping fraud*" (46), the chatbot identified the intentions related to online shopping alerts, investment fraud alerts, victims of fraud, and phishing by SMS (47). After the option of alert online shopping was chosen (48), the chatbot provided information regarding safe procedures for purchasing and paying for goods

Table 1. Evaluation questionnaire and results.

NQ		Question	No Expert	Expert	Global
Sociological characterization	***Resource Skills and Digital Security***				
	Q1	I know how to use computer resources and electronic devices.	3,54	4,06	3,80
	Q2	I know cybersecurity issues, the protection of electronic devices, and the provision of services via the Internet.	3,04	3,91	3,48
	Professional experience				
	Q3	I have professional experience in the following areas: Cybersecurity, Public Prosecutor or Judicial Magistracy, and Police. No experience in the areas indicated.	28	35	63
	Professional experience in mitigation actions				
	Q4	I have professional experience in investigating or mitigating phenomena related to cybercrime.	–	2,70	2,70
	Q5	I have professional experience in cybersecurity issues.	–	2,67	2,67
	Knowledge of computer crime and cybersecurity				
	Q6	I have a general knowledge of the various ways in which computer crime manifests itself.	2,50	4,11	3,31
	Q7	I have general knowledge of cybersecurity.	2,54	3,66	3,10
Users Perception	***Expectations about the identification and usefulness of the artifact's contents***				
	Q8	I identified the content I had always idealized on issues of computer crime awareness in the experience of using the infoCyberCrime chatbot.	3,46	3,89	3,70
	Q9	The information provided by the infoCyberCrime chatbot helps raise awareness of computer crime.	4,43	4,29	4,35
	Efficiency and Speed of Conversational Flows				
	Q10	InfoCyberCrime dialog flows and processing is fast and efficient.	4,29	4,23	4,25
	Suggestions for Research and Information Accessibility				
	Q11	The search suggestions provided by the infoCyberCrime chatbot make information more accessible.	4,43	4,43	4,43
	Q12	What number of search suggestions (text tags) would be ideal to make the infoCyberCrime chatbot more efficient in making content accessible? (with proposals 1 to 4).	3,18	3,09	3
	Personal Data, IT Security, Privacy and Ethics				
	Q13	I have no concerns about protecting personal data when using the infoCyberCrime chatbot.	3,89	3,89	3,89
	Q14	I did not observe any concerns about aspects related to computer security when using the infoCyberCrime chatbot.	4,04	4,23	4,14
	Q15	I did not raise any privacy concerns when using the infoCyberCrime chatbot.	3,89	4,11	4,02
	Q16	I have not observed any ethical issues or misinformation in the content provided by the infoCyberCrime chatbot.	4,04	4,31	4,19
	Q17	I realized that the content provided by the infoCyberCrime chatbot has a reliable and credible origin.	4,61	4,57	4,59
	Characteristics and suitability to implement the artifact				
	Q18	The infoCyberCrime chatbot has features suited to raising awareness of computer crime.	4,36	4,37	4,37
	Q19	The infoCyberCrime chatbot has features suitable for integration into public administration websites.	4,39	4,40	4,40
	Q20	The infoCyberCrime chatbot has features that improve communication between the State and citizens.	4,25	4,31	4,29
	Q21	The infoCyberCrime chatbot has suitable features for informing citizens of computer crime phenomena on public administration websites.	4,43	4,49	4,46
		Global (Q8-Q11 and Q13-Q21)	**4,19**	**4,27**	**4,24**

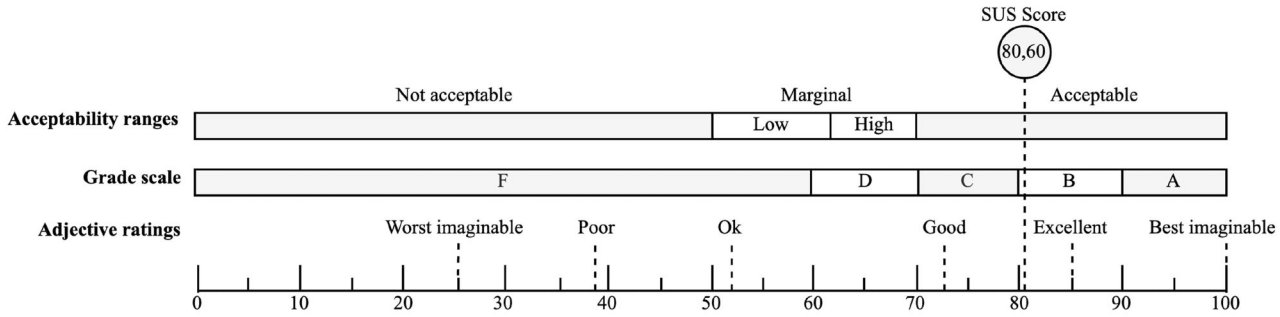

Figure 11. Interpretation of the system usability scale result. Adapted from Bangor et al. (2009).

in digital environments (50). In the fifth use case (Figure 10), the assistant was asked about a topic divergent from its purpose: "*Where can I buy a computer?*" (52). As this intention was not recognized, the assistant offered to rephrase the question or contact a human agent (phone or email) (53). As alternative channels, the possibility of using other conversational assistants was provided (53).

Despite the artifact's prototype condition at the end of the demonstration phase, it was efficient enough to implement the evaluation phase.

6. Prototype evaluation phase

The evaluation perspective applied, like Peras (2018), Creswell and Creswell (2018), and Cantador et al. (2021), was based on the mixed method, including qualitative and quantitative aspects, both in the data collection techniques and their treatment and interpretation. The evaluation dimension followed metrics of user perception during the experience of using the chatbot (Cantador et al., 2021; Nirala et al., 2022; Peras, 2018; Stamatis et al., 2020), as well as objective metrics generated by Watson Assistant during the evaluation process (de Lacerda & Aguiar, 2019; Höhn & Bongard-Blanchy, 2021; Nirala et al., 2022; Peras, 2018). The data relating to the first dimension of the evaluation was obtained through the survey data collection technique, using an electronic questionnaire in a structured mode and with closed answers (Creswell & Creswell, 2018; Jain et al., 2018; Peras, 2018). The questionnaire was applied to two groups of users, sociologically characterized as having (expert) or not having (non-expert) professional experience in mitigating computer crime and the cybersecurity sector. For the second aspect of the evaluation, the data was generated by the *Analytics* tool (IBM Cloud - Watson Assistant, n.d.b) from Watson Assistant (IBM, n.d.b), which summarizes all the metrics.

Considering the hypothetical vulnerability of some users due to their advanced age, the Ethics Committee of the University of Trás-os-Montes e Alto Douro (UTAD) was requested to provide an opinion on the research plan's conformity (CE-UTAD, n.d). Following the committee's positive feedback, potential participants in the evaluation process were recruited. The 63 participants, all over 16 years old, collaborated by sending the fully completed electronic questionnaire. Some participants come from professional groups in cybersecurity, police forces, and judicial members. The first group (28 participants) refers to users who need more experience using computer resources and cybersecurity rules and modes of action related to cybercrime (non-experts). The second group (35 participants) includes participants with experience using IT resources, cybersecurity, and computer crime methods (experts). The electronic questionnaire was designed in a structured format, with closed multiple-choice questions, using the Likert Scale method (Creswell & Creswell, 2018; Jain et al., 2018; Peras, 2018), with the following measurement: 1 - Strongly Disagree - (1.00 to 1.80); 2 - Disagree - (1.81 to 2.60); 3 - Neutral - (2.61 to 3.40); 4 - Agree - (3.41 to 4.20); 5 - Strongly Agree - (4.21 to 5.00).

Table 1 describes the first seven questions (Q1 to Q7) regarding the sociological characterization. The remaining questions (Q8 to 21) were intended to collect data on the user experience that the participants experienced during their interaction with the chatbot.

6.1. First strand of evaluation

Except for the sociological aspects (Q1 to Q7) and the appropriate number of accessibility suggestions (Q12), we proceeded (Table 1) to interpret the results regarding the perception of the user experience (Q8 to Q11 and Q13 to Q21). Overall, the participants rated the artifact with an average of 4.24 (total agreement). The non-expert participants averaged 4.19 (agreement). As for the experts, they valued the artifact with an average of 4.27 (total agreement).

The second part of the questionnaire evaluation concerns specific usability issues with the *System Usability Scale* application.

The final score translated into an overall value of 5080 points, corresponding to a final average of 80.63 points. As shown in Figure 11, according to the various ways of interpreting it (Bangor et al., 2009) in acceptable values (*acceptability range*), grade B (*grade scale*), or Good (*adjective rating*).

6.2. Second strand of evaluation

The data was collected during the interaction between the participants and the chatbot, using the *Overview* and *User Conversations* functionality in the *Analytics* tool of Watson Assistant. During the interaction between the participants and the chatbot, 843 messages were recorded, of which 795 (94.3%) were recognized. On the other hand, 48 messages

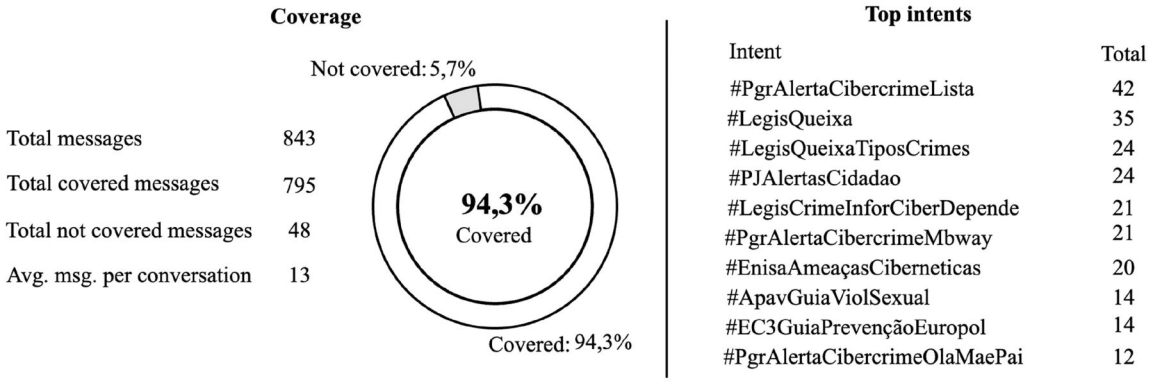

Figure 12. Results from the analytics tool.

(5.7%) did not associate the user's intention with any *intent* in the knowledge base. The *User Conversations* tool allows a detailed record of all the conversations and analysis patterns that influence the efficiency of the artifact itself.

As shown in Figure 12, the patterns identified in the efficiency concern accessibility factors alluding to the theme's suggestions in the assistant's initial interface. This efficiency was due to the many users who adhered to the topic suggestions on the artifact's initial interface without entering any text. After analyzing the results and user interactions, we improved the intent catalog with new user examples.

7. Conclusions

Although no studies were identified that addressed the role of chatbots in raising awareness of computer crime in specific public service sectors, the topic's relevance was noted by the interest and support of some State entities and other public bodies in studying the phenomenon. Factors to consider when designing, developing, and evaluating chatbot architectures in the context under study were identified. Concepts, research methodologies, technologies, architectural proposals, and evaluation techniques were applied in the artifact proposal's idealization, design, implementation, and evaluation. The demonstration phase aimed to determine the performance tests regarding the efficiency of conversational flows, especially the information available in various computer crime areas. The results of the first evaluation phase included 63 participants, 34 of whom had professional experience in areas related to the subject under investigation (experts). Overall (experts and non-experts), in the first part of the evaluation, the participants rated the artifact positively, reaching an average of 4.24 on a Likert agreement scale. The non-expert participants gave an average score of 4.19, while the expert participants gave an average of 4.27, further highlighting the artifact's various strengths. The final score for the SUS application resulted in an average of 80.63 (acceptable values, grade B or Good). Concerning the second part of the evaluation, which involved measuring objective and efficiency data in *analytics tools* from Watson Assistant, 843 messages were processed, of which 795 (94.3%) corresponded to content recognized and processed by the artifact. The data generated during the evaluation phase resulted in iterative processes of the artifact, covering accessibility factors, content in the knowledge base (intents and user examples), automatic learning processes, and resource scalability.

The research objective, related to designing, developing, and validating an artifact (chatbot) suitable for PA websites aimed at raising awareness of computer crime, is achieved. Although the artifact prototype condition is high, its architecture aligns with PA requirements. In addition to regulatory aspects, it incorporates resource scalability features and advanced computing functionalities.

7.1. Main contributions

Several innovative factors have been identified in various dimensions of the public sector in the field of awareness of computer crime, resulting in multiple contributions: (1) a computer crime awareness perspective based on innovative paradigms in emerging technologies in the public sector, such as AI and chatbots; (2) a validated artifact in multiple aspects with high levels of accessibility, usability, security, stability, scalability, and resource resilience, supported by a broad theoretical and practical base, to raise awareness of computer crime; (3) a proposal to organize diversified content based on government studies and reports on the incidence of computer crime to implement them in conversational assistant and reach a varied target audience; (4) a proposal for institutional electronic cooperation and interoperability between the entities responsible for mitigating and investigating computer crime, in terms of sharing knowledge to create contents, who must be professional based, credible, and endowed with ethical principles. This study makes a significant contribution by identifying the overall context that characterizes the proposed artifact's suitability, usefulness, and efficiency, even at a prototype stage.

7.2. Research limitations

The limitations of this study stem from the necessity for further research on utilizing chatbots in public administration to raise awareness of computer crime. The literature review underscored the scarcity of studies to develop and access conversational assistants for this purpose. Moreover, the study's emphasis on the public context resulted in the exclusion of solutions designed for other areas, such as industry and commerce.

Watson Assistant's free and basic plan limited the idealization of the chatbot's architecture, hindering the optimization and implementation of components and tools that could enhance its operation in the field of interoperability. It highlighted challenges in the collaboration between public entities responsible for mitigating and investigating crime in Portugal, such as the Public Prosecutor's Office, the Judicial Police, and the National Cybersecurity Center. These restrictions have particularly affected creating and disseminating awareness-raising content regarding these criminal issues and threats.

While the selection of participants was methodologically rigorous, involving professionals in computer crime mitigation and cybersecurity, active aging center users, university seniors, and the general public, the sample of 63 participants may present a limitation. This small sample size might not adequately represent the results, particularly for groups with lower digital literacy, potentially affecting the generalization of findings. Moreover, the lack of a comprehensive demographic analysis- covering variables such as age and prior experience with cybercrime- could influence users' perception of the chatbot's effectiveness. Therefore, future investigations should include broader and more diverse samples to produce more representative conclusions. Additionally, overcoming technological limitations by adopting more advanced and interoperable models will be essential to enhancing the use of chatbots to raise awareness of digital security and empower citizens against computer crime threats.

7.3. Future research

Considering the encouraging research outcomes, upcoming efforts should concentrate on deploying chatbots in practical applications within the public sector. This will emphasize the necessity of enhancing awareness of their effectiveness, particularly within the public justice system. Future research must focus on critical areas like pinpointing current research gaps and improving the design and evaluation of chatbots. Important factors such as implementation, interoperability, knowledge scalability for users, and technical constraints should be considered to maximize the impact of these initiatives' technologies.

These chatbots should be carefully designed as effective tools to raise awareness of computer crime. To achieve this, it is essential to involve specialized public bodies such as the Public Prosecutor's Office, the Judicial Police, the National Cybersecurity Centre, and other relevant entities. Strategies that promote the optimization and interoperability of resources among public entities should be implemented, considering the diversity of criminal phenomena and target audiences. The development of specialized content should occur in collaboration with organizations like the Portuguese Association for Victim Support and the Safe Internet Center, ensuring that chatbots provide accurate, up-to-date, and relevant information. Integrating chatbots into these institutions' channels will enhance their response to cyber threats.

Establishing a robust technological infrastructure is imperative for the successful implementation of chatbots. Strategic planning must encompass technical components, including the hosting environment and system architecture. Tools such as the IBM Language Translator API can provide multilingual support, thereby expanding the reach of chatbots and enhancing their accessibility to diverse populations. This methodology bolsters the adaptive capacity of public entities, facilitating an increased efficiency ecosystem.

The governance and management factors are essential to chatbots' long-term success. Implementing effective governance mechanisms guided by user interactions and feedback is crucial to ensure ongoing enhancements. Such mechanisms will improve the functionalities of chatbots and guarantee their alignment with strategic digital security objectives, including data protection and threat detection. The adoption of agile and data-driven management practices will be necessary for adapting chatbots to evolving threats, emerging technologies, and the specific needs of target audiences. Furthermore, evaluating the effectiveness of chatbots and the relevance of their content is a significant area for future research. In addition, continuous data collection- encompassing user feedback, behavior analysis, and trend monitoring- will facilitate identifying knowledge gaps and refining public policies, thereby enhancing the efficacy of computer crime prevention and response initiatives. Despite promising experimental results, the necessity to assess the fundamental behavioral changes produced by interactions with chatbots has been underscored. Future studies should incorporate longitudinal assessments to evaluate lasting improvements in cybersecurity awareness, user decision-making, and long-term knowledge retention. These evaluations will enhance our understanding of how chatbots influence user behavior and contribute to their ongoing improvement effectiveness.

As outlined in the limitations section, despite the study adhering to rigorous selection criteria and encompassing a diverse array of participant profiles, the sample size of 63 individuals may constrain representativeness, notably among users exhibiting lower digital literacy. Consequently, future research endeavors should strive to enlarge the sample size by incorporating a broader and more heterogeneous population, thereby facilitating a more comprehensive evaluation of the impact of chatbots across various user demographics. Furthermore, an in-depth demographic analysis should be conducted to assess how variables such as digital skillset and familiarity with technology affect the adoption and overall effectiveness of chatbots.

With the rapid advancement of conversational assistant technologies, particularly OpenAI's ChatGPT, it is essential to explore tools that enhance the architecture of chatbots. These generative and probabilistic tools should ensure data protection, information technology security, auditing, and compliance with ethical standards. Large Language Models (LLMs) offer significant potential to improve the efficacy of chatbots, especially when customized and trained using specialized datasets in areas such as computer crime and cybersecurity.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work is funded by national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., under the support UID/50014/2023 (https://doi.org/10.54499/UID/50014/2023).

ORCID

Luís Pimentel http://orcid.org/0000-0002-0810-8601
Maria do Rosário Bernardo http://orcid.org/0000-0002-9518-0854
Tânia Rocha http://orcid.org/0000-0002-2605-9284

References

Adamopoulou, E., & Moussiades, L. (2020). Chatbots: History, technology, and applications. *Machine Learning with Applications*, *2*(July), 100006. https://doi.org/10.1016/j.mlwa.2020.100006

Agência para a Modernização Administrativa. (n.d). *Página Inicial - acessibilidade.gov.pt*. [Online]. https://www.acessibilidade.gov.pt/

Akkaya, C., & Krcmar, H. (2019). *Potential use of digital assistants by governments for citizen services: The case of Germany* [Paper presentation]. ACM International Conference Proceeding Series, in dg.o 2019. New York, NY, USA: Association for Computing Machinery (pp. 81–90). https://doi.org/10.1145/3325112.3325241

Androutsopoulou, A., Karacapilidis, N., Loukis, E., & Charalabidis, Y. (2019). Transforming the communication between citizens and government through AI-guided chatbots. *Gov Inf Q*, *36*(2), 358–367. https://doi.org/10.1016/j.giq.2018.10.001

Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, *35*, 100398. https://doi.org/10.1016/j.dcm.2020.100398

Antoniadis, P., & Tambouris, E. (2021). *PassBot: A chatbot for providing information on Getting a Greek Passport* [Paper presentation]. ACM International Conference Proceeding Series, in ICEGOV '21. New York, NY, USA: Association for Computing Machinery (pp. 292–297). https://doi.org/10.1145/3494193.3494233

Antoniadis, P., & Tambouris, E. (2022). *PassBot: A Chatbot for providing information on getting a greek passport* [Paper presentation]. Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance in ICEGOV '21. New York, NY, USA: Association for Computing Machinery (pp. 292–297). https://doi.org/10.1145/3494193.3494233

Aoki, N. (2020). An experimental study of public trust in AI chatbots in the public sector. *Gov Inf Q*, *37*(4), 101490. https://doi.org/10.1016/j.giq.2020.101490

APAV. (n.d). *Associação Portuguesa de Apoio à Vítima*. APAV. [Online]. https://apav.pt/apav_v3/index.php/pt/apav-1/quem-somos

ARRS - Slovenian Research (2022). *Annual Report on Internal Security (ARIS 2022)*. https://www.aris-rs.si/en/gradivo/dokum/inc/23/LP-ARRS-2022-eng.pdf

Assembly of the Republic (2009). Law No. 109/2009 of 15 September 2009 (Cybercrime Law). *Official Journal of the European Union, 165/2008*, n.o série i of 2008-08-27, 6038–6042.

Banco de Portugal. (n.d). *Missão e funções | Banco de Portugal*. BdP. [Online]. https://www.bportugal.pt/pagina/missao-e-funcoes

Bang, J., Kim, S., Nam, J. W., & Yang, D. G. (2021). *Ethical Chatbot design for reducing negative effects of biased data and unethical conversations* [Paper presentation]. 2021 International Conference on Platform Technology and Service, PlatCon 2021 - Proceedings. https://doi.org/10.1109/PlatCon53246.2021.9680760

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *Int J Hum Comput Interact*, *24*(6), 574–594. https://doi.org/10.1080/10447310802205776

Bangor, A., Kortum, P., & Miller, J. (2009). Determining what individual SUS scores mean; adding an adjective rating. *J Usability Stud*, *4*(3), 114–123.

Banire, B., Al Thani, D., & Yang, Y. (2021). *Addressing cyber security accessibility: A qualitative study* [Paper presentation].34th British HCI workshop and doctoral consortium 34 (pp. 1–5). https://doi.org/10.14236/ewic/HCI2021-W5.2

Barbara, A., & Stuart, C. K. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical Report, Ver. 2.3 EBSE Technical Report. EBSE*, *1*(January 2007), 1–54.

Beris, T., Lampathaki, F., Moumtzi, V., & Askounis, D. (2019). *Towards a decentralized, trusted, intelligent and linked public sector: A report from the Greek trenches* [Paper presentation]. The Web Conference 2019 - Companion of the World Wide Web Conference, WWW 2019, in WWW '19. New York, NY, USA: Association for Computing Machinery (pp. 840–849). https://doi.org/10.1145/3308560.3317077

Borsci, S., Malizia, A., Schmettow, M., van der Velde, F., Tariverdiyeva, G., Balaji, D., & Chamberlain, A. (2022). The Chatbot usability scale: The design and pilot of a usability scale for interaction with AI-based conversational agents. *Personal and Ubiquitous Computing*, *26*(1), 95–119. https://doi.org/10.1007/s00779-021-01582-9

Budiman, M. A., & Aminanto, M. E. (2022). Use of Intelligence Based Agents to Deal with Cyber Crime. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, *5*(1), 3679–3685. https://doi.org/10.33258/birci.v5i1.4049

Burnes, D., Henderson, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American Journal of Public Health*, *107*, e13–e21. https://doi.org/10.2105/AJPH.2017.303821

Cantador, I., Viejo-Tardío, J., Cortés-Cediel, M. E., & Rodríguez Bolívar, M. P. (2021). *A Chatbot for searching and exploring open data: implementation and evaluation in e-government* [Paper presentation]. ACM international conference proceeding series (pp. 168–179). https://doi.org/10.1145/3463677.3463681

Carvalho, J. V., Carvalho, S., & Rocha, Á. (2020). European strategy and legislation for cybersecurity: Implications for Portugal. *Cluster Computing*, *23*(3), 1845–1854. https://doi.org/10.1007/s10586-020-03052-y

Centro de Internet Segura. (n.d). *O Centro de Sensibilização | Internet Segura*. CIS. [Online]. https://www.internetsegura.pt/cis/centro-de-sensibilizacao

Centro Nacional de Cibersegurança (2021). *Cibersegurança em Portugal - Relatório Riscos & Conflitos*. [Online]. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf

Centro Nacional de Cibersegurança. (n.d). *Observatório de Cibersegurança*. Observatório de Cibersegurança. [Online]. https://www.cncs.gov.pt/pt/observatorio/#relatorios

CE-UTAD (n.d). *Comissão de Ética da UTAD*. https://www.utad.pt/ce-utad/

Chaves, A. P., & Gerosa, M. A. (2021). How should my chatbot interact? A survey on social characteristics in human–chatbot interaction design. *Int J Hum Comput Interact*, *37*(8), 729–758. https://doi.org/10.1080/10447318.2020.1841438

Cheng, Y., & Jiang, H. (2020). How do AI-driven Chatbots impact user experience? examining gratifications, perceived privacy risk, satisfaction, loyalty, and continued use. *J Broadcast Electron Media*, *64*(4), 592–614. https://doi.org/10.1080/08838151.2020.1834296

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health: CP & EMH*, *16*(1), 24–35. https://doi.org/10.2174/1745017902016010024

Corea, C., Delfmann, P., & Nagel, S. (2020). *Towards intelligent chatbots for customer care - Practice-based requirements for a research agenda* [paper presentation]. Proceedings of the Annual Hawaii International Conference on System Sciences, vol. 2020-Janua (pp. 5819–5828), https://doi.org/10.24251/hicss.2020.713

Creswell, J. W., & Creswell, J. D. (2018). *Research Defign: Qualitative, Quantitative, and Mixed M ethods Approaches*. SAGE Publications.

Dan, A., Gupta, S., Rakshit, S., & Banerjee, S. (2019). *Toward an AI Chatbot-Driven advanced digital locker: EHaCON 2018, Kolkata, India* (pp. 37–46). https://doi.org/10.1007/978-981-13-1544-2_4

Daniel, G., Cabot, J., Deruelle, L., & Derras, M. (2020). Xatkit: A multimodal low-code chatbot development framework. *IEEE Access*, *8*, 15332–15346. https://doi.org/10.1109/ACCESS.2020.2966919

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, *38*(3), 475–487., doi: . https://doi.org/10.1006/imms.1993.1022

de Andrade, G. G., Silva, G. R. S., Júnior, F. C. M. D., Santos, G. A., de Mendonça, F. L. L., & de Sousa, R. T. (2020). *EvaTalk: A chatbot system for the brazilian government virtual school* [Paper presentation]. ICEIS 2020 - Proceedings of the 22nd International Conference on Enterprise Information Systems (pp. 556–562). https://doi.org/10.5220/0009418605560562

de Lacerda, A. R. T., & Aguiar, C. S. R. (2019). *FLOSS FAQ Chatbot project reuse: How to allow nonexperts to develop a chatbot* [Paper presentation]. Proceedings of the 15th International Symposium on Open Collaboration in OpenSym '19. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3306446.3340823

DECO PROteste. (n.d.) *Quem somos e o que fazemos | DECO PROteste*. DECO. [Online]. https://www.deco.proteste.pt/info/os-nossos-servicos/quem-somos

de Melo, D. N. A., & I. T., Monteiro. (2021). Communication and Personality: How COVID-19 government chatbots express themselves [Paper presentation]. ACM International Conference Proceeding Series, in IHC '21. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3472301.3484362

do Rosário Valverde, M. S., & Couto e Vasconcelos, A. F. F. (2019). Chatbot in the online provision of government services. *Atas da Conferencia da Associação Portuguesa de Sistemas de Informação*.

EC3. (n.d). *European Cybercrime Centre - EC3 | Europol*. Europol. [Online]. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

El Hajal, G., Abi Zeid Daou, R., & Ducq, Y. (2021). *Human firewall: Cyber awareness using WhatApp AI Chatbot* [Paper presentation]. 2021 IEEE 3rd International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 66–70). https://doi.org/10.1109/IMCET53404.2021.9665642

El Hajal, G., Daou, R. A. Z., & Ducq, Y. (2021). *Human firewall: Cyber awareness using WhatApp AI chatbot* [Paper presentation].2021 IEEE 3rd International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 66–70). https://doi.org/10.1109/IMCET53404.2021.9665642

ENISA (2024). *The European Union Agency for Cybersecurity - ENISA*. ENISA. [Online]. https://www.enisa.europa.eu/about-enisa

European Commission (2010). *EIS - European Interoperability Strategy*. [Online]. http://ec.europa.eu/idabc/en/document/7772.html

European Commission (2013). *Core Public Service Vocabulary (CPSV)*. [Online]. https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/core-public-service-vocabulary

European Commission (2016). *EU eGovernment Action Plan 2016-2020 - Accelerating the Digital Transformation of Government*. COM(2016) 179 final no. 179 [Online]. https://ec.europa.eu/isa2/sites/default/files/docs/publications/eu-egovernment-action-plan-2016-2020_en.pdf

European Commission (2017). *New European Interoperability Framework: Promoting seamless services and data flows for European public administrations*. White Pages, [Online]. https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

European Commission (2019a). *Architecture for public service chatbots (ISA2 Program). Directorate-General for Informatics*[Online]. https://joinup.ec.europa.eu/sites/default/files/news/2019-09/ISA2_Architecture for public service chatbots.pdf

European Commission (2019b). *The European cloud strategy, no. May* (pp 6–8). [Online]. https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en

European Commission (2020a). Recommendations for organizing and governing integrated public services. *Publication Office of the European Union* [Online]. https://op.europa.eu/en/publication-detail/-/publication/717f26a7-722b-11ea-a07e-01aa75ed71a1/language-en/format-PDF/source-281286075

European Commission (2020b). *The EU's cybersecurity strategy for the digital decade. Shaping Europe's digital future*[Online]. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission (2021a). Coordinated plan on artificial intelligence 2021 review. *Shaping Europe's digital future*[Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

European Commission (2021b). *European standard EN 301 549 V3.2.1, Accessibility requirements for ICT products and services.* [Online]. https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf

European Commission, (2018). *Ethics guidelines for trustworthy AI*. Futurium [Online]. https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html

European Parliament (2021a). *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*. [Online]. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

European Parliament (2021b). Framework of ethical aspects of artificial intelligence, robotics and related technologies. *Official Journal of the European Union*, *C 404*, 63–106. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020IP0275

European Parliament and of the council (2016). Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies. *Jornal Oficial da União Europeia*, *L 327*, 1–15. https://data.europa.eu/eli/dir/2016/2102/oj

European Parliament and the Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union and Available in EUR-Lex*, *L 119*, 1–88. https://data.europa.eu/eli/reg/2016/679/oj

European Parliament and the Council of the European Union (2018). *Artificial Intelligence for Europe: Communication from the Commission*. EUR-Lex, [Online]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN

Fenge, L. A., & Lee, S. (2018). Understanding the risks of financial scams as part of elder abuse prevention. *The British Journal of Social Work*, *48*(4), 906–923. https://doi.org/10.1093/bjsw/bcy037

Filipe, L., Gomes, O., Doutoral, P., Digitais, M., João, O., Tavares, M. R. S. (2012). *Influência da Perceção Humana no Processo de Visualização de Dados Seminário de Investigação* (p. 37). https://web.fe.up.pt/~tavares/downloads/publications/relatorios/Seminario_VF_LeandroGomes.pdf

Gaggi, O., & Perinello, L. (2022). *Improving accessibility of web accessibility rules* [Paper presentation]. Proceedings of the 2022 ACM Conference on Information Technology for Social Good in GoodIT '22. New York, NY, USA: Association for Computing Machinery (pp. 167–174). https://doi.org/10.1145/3524458.3547267

Gerontas, A. (2020). *Towards an e-Government semantic interoperability assessment framework* [Paper presentation]. Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance in ICEGOV '20. New York, NY, USA: Association for Computing Machinery (pp. 767–774). https://doi.org/10.1145/3428502.3428617

Hamad, S., & Yeferny, T. (2020). A chatbot for information security. *IJCSNS International Journal of Computer Science and Network Security*, *20*(4), 287–291., [Online] Available: https://arxiv.org/abs/2012.00826

Hari Prasad, D., & Vijayakumar, V. (2021). Intelligent Chatbot development for text based cyberbullying prevention. *International Journal of New Innovations in Engineering and Technology*, *17*(1), 73–81.

Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., Snášel, V., & Ogiela, L. (2021). Chatbots: Security, privacy, data protection, and social aspects. *Concurr Comput*, *33*(19), e6426. https://doi.org/10.1002/cpe.6426

Hasan, I., Rizvi, S., Jain, S., & Huria, S. (2021). *The AI enabled Chatbot framework for intelligent citizen-government interaction for delivery of services* [Paper presentation]. 2021 8th International Conference

on Computing for Sustainable Global Development (INDIACom) (pp. 601–606).

Hatsue, E., Huzita, M., Marci, H., Oliveira, D., & Marcos, J. (2000). A proposal of agent-based software architecture. *Acta Scientiarum - Technology*, *22*(5), 1339–1346. https://doi.org/10.4025/actascitechnol.v22i0.3131

He, J., & Xin, C. (2021). Developing an AI-powered chatbot to support the administration of middle and high school cybersecurity camps. *Journal of Cybersecurity Education, Research and Practice*, *2021*(1), 6. https://doi.org/10.62915/2472-2707.1077

Henman, P. (2020). Improving public services using artificial intelligence: Possibilities, pitfalls, governance. *Asia Pacific Journal of Public Administration*, *42*(4), 209–221. https://doi.org/10.1080/23276665.2020.1816188

Hevner, A., & Storey, V. (2023). Research challenges for the design of Human-Artificial Intelligence Systems (HAIS). *ACM Transactions on Management Information Systems*, *14*(1), 1–18. https://doi.org/10.1145/3549547

Hevner, March, Park, Ram. (2004). Design science in information systems research. *Management Information Systems Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Höhn, S., & Bongard-Blanchy, K. (2021). Heuristic evaluation of COVID-19 chatbots. In A. Følstad, T. Araujo, S. Papadopoulos, E. L.-C. Law, E. Luger, M. Goodwin, & P.r B. Brandtzaeg (Eds.), *Chatbot Research and Design. CONVERSATIONS 2020. Lecture Notes in Computer Science* (Vol. 12604). Springer. https://doi.org/10.1007/978-3-030-68288-0_9

Huang, J. M., Stringhini, G., & Yong, P. (2015). Quit playing games with my heart: Understanding online dating scams. In M. Almgren, V. Gulisano, & F. Maggi (Eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science* (Vol. 9148). Springer. https://doi.org/10.1007/978-3-319-20550-2_12

Hufnagel, S., Moiseienko, A. (Eds.). (2019). *Criminal Networks and Law Enforcement: Global Perspectives On Illegal Enterprise* (1st ed.). Routledge. https://doi.org/10.4324/9781351176194

IBM (n.d.a). *Conversational chatbot architecture: Reference diagram*. Cloud Architecture Center. [Online]. https://www.ibm.com/cloud/architecture/architectures/cognitiveConversationDomain/reference-architecture/

IBM (n.d.b). *Watson assistant (Virtual Agent)*. Watson Assistant. [Online]. https://www.ibm.com/products/watsonx-assistant

IBM Cloud - Watson Assistant (n.d.a). Building a complex dialog | IBM Cloud Docs. IBM Cloud. [Online]. https://cloud.ibm.com/docs/assistant?topic=assistant-tutorial

IBM Cloud - Watson Assistant (.n.d.b). *IBM Chatbot analytics*. IBM Products. [Online]. https://www.ibm.com/products/watsonx-assistant/analytics

IBM Cloud - Watson Discovery (n.d). *IBM Watson discovery*. IBM Products. [Online]. https://www.ibm.com/products/watson-discovery

IBM Cloud - Watsonx Assistant (n.d). *Watsonx Assistant | IBM Cloud Docs*. IBM Cloud. [Online]. https://cloud.ibm.com/docs/watson-assistant?topic=watson-assistant-welcome-new-assistant

IBM Cloud (n.d.a). *Adding the web chat to your website | Classic Watson Assistant*. IBM Cloud Docs. [Online]. https://cloud.ibm.com/docs/assistant?topic=assistant-deploy-web-chat

IBM Cloud (n.d.b). *Adding the web chat to your website | IBM Cloud Docs*. IBM Cloud Docs. [Online]. https://cloud.ibm.com/docs/assistant?topic=assistant-deploy-web-chat

International Organization for Standardization. (2005). *ISO/IEC 27001 and related standards—Information security management*. [Online]. https://www.iso.org/isoiec-27001-information-security.html

Jain, M., Kumar, P., Kota, R., & Patel, S. N. (2018). *Evaluating and informing the design of chatbots* [paper presentation]. DIS 2018 - Proceedings of the 2018 Designing Interactive Systems Conference (pp. 895–906). https://doi.org/10.1145/3196709.3196735

Kalache, A., & Gatti, A. (2003). Active ageing: A policy framework. *Advances in Gerontology = Uspekhi Gerontologii/Rossiiskaia Akademiia Nauk, Gerontologicheskoe Obshchestvo*, *11*, 7–18. https://doi.org/10.1080/tam.5.1.1.37

Khokhawat, S., Jain, I., Shekhar, G., Choudhary, S., & Narooka, P. (2021). Efficient Chatbot for crime awareness system. *International Research Journal of Modernization in Engineering Technology and Science*, *3*(5), 3830–3835.

Kowalski, S., Pavlovska, K., & Goldstein, M. (2013). Two case studies in using chatbots for security training. In R. C. Dodge and L. Futcher (Eds.), *Information Assurance and Security Education and Training* (pp. 265–272). Springer Berlin Heidelberg.

Kumar, C., & Mukund, C. M. (2020). A review of select innovations and emerging trends in E-governance. *International Journal of Research in Engineering, Science and Management*, *3*(8), 65–74.

Laorden, C., Galán-García, P., Santos, I., Sanz, B., Hidalgo, J. M. G., & Bringas, P. G. (2013). Negobot: A conversational agent based on game theory for the detection of paedophile behaviour. In Á. Herrero, V. Snasel, A. Abraham, I. Zelinka, B. Baruque, H. Quintián, J. Calvo, J. Sedano, & E. Corchado (Eds.), *International Joint Conference CISIS'12-ICEUTE'12-SOCO'12 Special Sessions. Advances in Intelligent Systems and Computing* (Vol. 189). Springer. https://doi.org/10.1007/978-3-642-33018-6_27

Leaua, C., & Didu, I.-A. (2021). Chatbots. Legal challenges and the Eu legal policy approach. *Perspectives of Law and Public Administration*, *10*(3), 210–222.

Lee, S., Lee, J., Lee, W., Lee, S., Kim, S., & Kim, E. T. (2020). Design of integrated messenger anti-virus system using Chatbot service. *2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South)* (pp. 1613–1615). https://doi.org/10.1109/ICTC49870.2020.9289514

Mahmoud, M., & Kumar, R. (2020). A review on Chatbot design and implementation techniques. *International Research Journal of Engineering and Technology (IRJET)*, *7*(2), 2791.

Manzoor, A., & Jannach, D. (2021). Conversational recommendation based on end-to-end learning: How far are we? *Computers in Human Behavior Reports*, *4*, 100139. https://doi.org/10.1016/j.chbr.2021.100139

Maragno, G., Tangi, L., Gastaldi, L., & Benedetti, M. (2023). AI as an organizational agent to nurture: Effectively introducing chatbots in public entities. *Public Management Review*, *25*(11), 2135–2165. https://doi.org/10.1080/14719037.2022.2063935

Martins, A. I., Rosa, A. F., Queirós, A., Silva, A., & Rocha, N. P. (2015). European Portuguese validation of the System Usability Scale (SUS). *Procedia Computer Science*, *67*, 293–300. https://doi.org/10.1016/j.procs.2015.09.273

Ministério Público. (n.d). *Portal do Ministério Público - Crime*. Os tipos de crimes. [Online]. https://www.ministeriopublico.pt/perguntas-frequentes/crime

Misuraca, G., Van Noordt, C., & Boukli, A. (2020). *The use of AI in public services: Results from a preliminary mapping across the EU* [Paper presentation]. ACM International Conference Proceeding Series in ICEGOV '20. New York, NY, USA: Association for Computing Machinery (pp. 90–99). https://doi.org/10.1145/3428502.3428513

Monteiro, L. H. D. A., Rodrigues, C. M. D. O., & De Sousa, A. M. C. (2022). *an information system for law integrating ontological bases with a legal reason*er Chatbot [Paper presentation]. ACM International Conference Proceeding Series, in SBSI, vol. Par F18047. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3535511.3535555

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, *23*(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Murcia Triviño, J., Moreno Rodríguez, S., Díaz López, D. O., & Gómez Mármol, F. (2019). *C3-Sex: A Chatbot to chase cyber perverts* [Paper presentation]. 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 50–57). https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00024

National Cyber Security Centre (NCSC) (2022). *Cybersecurity in Portugal - Risks and Conflicts Report - 3rd Edition*. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

National Cyber Security Centre (NCSC) (n.d). *Society 2020 report*. https://www.cncs.gov.pt/pt/relatorio-sociedade-2020/

Nirala, K. K., Singh, N. K., & Purani, V. S. (2022). A survey on providing customer and public administration based services using AI: Chatbot. *Multimedia Tools and Applications*, *81*(16), 22215–22246. https://doi.org/10.1007/s11042-021-11458-y

Oliveira, D., et al. (2017). *Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing* [Paper presentation]. https://doi.org/10.1145/3025453.3025831

OpenAI. (n.d). ChatGPT. https://chatgpt.com/gpts

Osakwe, J., Mutelo, S., & Shilamba, M. (2021). *Artificial Intelligence: A Veritable Tool for Governance in Developing Countries* [Paper presentation]. 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC) (pp. 1–6). https://doi.org/10.1109/IMITEC52926.2021.9714584

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peras, D. (2018). "©," *Economic and Social Development: Book of Proceedings* (pp. 89–97).

Petriv, Y., Erlenheim, R., Tsap, V., Pappel, I., & Draheim, D. (2020). Designing effective chatbot solutions for the public sector: A case study from Ukraine. *Communications in Computer and Information Science*, *1135*, 320–335. https://doi.org/10.1007/978-3-030-39296-3_24

Piccolo, L. S. G., Troullinou, P., & Alani, H. (2021). *Chatbots to Support Children in Coping with Online Threats: Socio-technical Requirements* [Paper presentation]. DIS 2021 - Proceedings of the 2021 ACM Designing Interactive Systems Conference: Nowhere and Everywhere in DIS '21. New York, NY, USA: Association for Computing Machinery (pp. 1504–1517). https://doi.org/10.1145/3461778.3462114

Pimentel, L. (n.d). *infoCyberCrime Chatbot*. [Online]. https://infocybercrime.s3.ams03.cloud-object-storage.appdomain.cloud/infoCyberCrime/index.html

Polícia Judiciária. (n.d). *Missão – Polícia Judiciária*. Polícia Judiciária. [Online]. https://www.policiajudiciaria.pt/missao/

Presidency of the Council of Ministers (2018). Resolution of the council of ministers no. 26/2018, of 8 March (INCoDe.2030). *Official Journal no. 48/2018, Series I of 2018-03-08*, 1207–1209.

Reis, J., & Melao, N. (2023). E-Democracy: Artificial Intelligence, Politics and State Modernization. *Proelium*, *VIII*(January), 399–432.

Reis, J., Santo, P., & Melão, N. (2020). Artificial intelligence research and its contributions to the European Union's political governance: Comparative study between member states. *Soc Sci*, *9*(11), 207. https://doi.org/10.3390/socsci9110207

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, *20*(3), 324–337. https://doi.org/10.1108/JFC-03-2013-0014

Rita, M. N., & Shava, F. B. (2021). *Chatbot driven web-based platform for online safety and sexual exploitation awareness and reporting in Namibia* [Paper presentation]. icABCD 2021 - 4th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, Proceedings (pp. 1–5). https://doi.org/10.1109/icABCD51485.2021.9519375

Santos, G. A., de Andrade, G. G., Silva, G. R. S., Duarte, F. C. M., Da Costa, J. P. J., & de Sousa, R. T. (2022). A conversation-driven approach for Chatbot management. *IEEE Access*, *10*, 8474–8486. https://doi.org/10.1109/ACCESS.2022.3143323

Sedoc, J., Ippolito, D., Kirubarajan, A., Thirani, J., Ungar, L., & Callison-Burch, C. (2019). *ChatEval: A tool for chatbot evaluation* [Paper presentation]. Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics (Demonstrations), Association for Computational Linguistics (pp. 60–65). http://aclweb.org/anthology/N19-4011

Simonsen, L., Steinstø, T., Verne, G., & Bratteteig, T. (2020). I'm disabled and married to a foreign single mother. Public service chatbot's advice on citizens' complex lives. *Electronic Participation. ePart 2020. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 12220). https://doi.org/10.1007/978-3-030-58141-1_11

Singh, K. (2011). Increment of cyber crimes against our securities. *JCEM International Journal of Computational Engineering & Management ISSN*, *12*(April), 116–120.

Sivcevic, D., Kosanin, I., Nedeljkovic, S., Nikolic, V., Kuk, K., & Nogo, S. (2020). *Possibilities of used intelligence based agents in instant messaging on e-government services* [Paper presentation]. 2020 19th International Symposium INFOTEH-JAHORINA, INFOTEH 2020 - Proceedings, no. Marchpp (pp. 18–20). https://doi.org/10.1109/INFOTEH48170.2020.9066343

Srivastava, S., Srivastava, K., & Arora, N. (2020). Exploration of a solution-centric crime awareness tool. *International Journal of Computer Applications*, *175*(22), 26–32. https://doi.org/10.5120/ijca2020920743

Stamatis, A., Gerontas, A., Dasyras, A., & Tambouris, E. (2020). Using chatbots and life events to provide public service information [Paper presentation]. ACM International Conference Proceeding Series, in ICEGOV '20. New York, NY, USA: Association for Computing Machinery (pp. 54–61). https://doi.org/10.1145/3428502.3428509

Susar, D., & Aquaro, V. (2019). *Artificial intelligence: Opportunities and challenges for the public sector* [Paper presentation]. ACM International Conference Proceeding Series in ICEGOV '19, vol. Part F1481. New York, NY, USA: Association for Computing Machinery (pp. 418–426). https://doi.org/10.1145/3326365.3326420

Tambouris, E., & Tarabanis, K. (2021). Towards Inclusive Integrated Public Service (IPS) Co-Creation and Provision [Paper presentation]. ACM International Conference Proceeding Series, in DG.O'21. New York, NY, USA: Association for Computing Machinery (pp. 458–462). https://doi.org/10.1145/3463677.3463726

Tao, C., Longya, R., & Xian, G. (2019). *AI innovation for advancing public service: The case of China's first Administrative Approval Bureau* [Paper presentation]. ACM International Conference Proceeding Series, in dg.o 2019. New York, NY, USA: Association for Computing Machinery (pp. 100–108). https://doi.org/10.1145/3325112.3325243

Tatarinova, L. F., Shakirov, K. N., & Tatarinov, D. V. (2016). Criminological analysis of determinants of cybercrime technologies. *Mathematics Education*, *11*(5), 1127–1134.

Tavanapour, N., Poser, M., & Bittner, E. A. C. (2020). Supporting the idea generation process in citizen participation - Toward an interactive system with a conversational agent as facilitator [Paper presentation]. 27th European Conference on Information Systems - Information Systems for a Sharing Society, ECIS 2019.

The European Parliament (2020). *Intellectual property rights for the development of artificial intelligence technologies (A9-0176/2020)*. [Online]. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html

The Presidency of the Council of Ministers (2019). Order No. 1088/2019, of 31 January (QDRCD-DigCom 2.1). *Official Journal, 22/2019, n.o série ii de 2019-01-31*, 4184–4186.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine*, *169*(7), 467–473. https://doi.org/10.7326/M18-0850

Ubaldi, B., Le Fevre, E. M., Petrucci, E., Marchionni, P., Biancalana, C., Hiltunen, N., Intravaia, D. M., & Yang, C. (2019). State of the art in the use of emerging technologies in the public sector. *OECD Working Papers on Public Governance 31*, OECD Publishing. https://doi.org/10.1787/932780bc-en

Ubowska, A., & Królikowski, T. (2022). Building a cybersecurity culture of public administration system in Poland. *Procedia Computer Science*, *207*, 1242–1250. https://doi.org/10.1016/j.procs.2022.09.180

Usability.gov. (n.d). *System Usability Scale (SUS).* [Online]. https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

van Noordt, C., & Misuraca, G. (2019). New wine in old bottles: Chatbots in government: exploring the transformative impact of chatbots in public service delivery. In P. Panagiotopoulos, N. Edelmann, O. Glassey, G. Misuraca, P. Parycek, T. Lampoltshammer, & B. Re (Eds.), *Electronic Participation. ePart 2019. Lecture Notes in Computer Science* (Vol. 11686). Springer. https://doi.org/10.1007/978-3-030-27397-2_5

van Noordt, C., & Misuraca, G. (2022). Artificial intelligence for the public sector: Results of landscaping the use of AI in government across the European Union. *Gov Inf Q*, *39*(3), 101714. https://doi.org/10.1016/j.giq.2022.101714

Vassilakopoulou, P., Haug, A., Salvesen, L. M., & Pappas, I. O. (2023). Developing human/AI interactions for chat-based customer services: Lessons learned from the Norwegian government. *European Journal of Information Systems*, *32*(1), 10–22. https://doi.org/10.1080/0960085X.2022.2096490

Villatoro-Tello, E., Callejas-Rodriguez, Á., Meza, I., & Ramirez-de-la-Rosa, G. (2016). *From dialogue corpora to dialogue systems: Generating a Chatbot with teenager personality for preventing cyber-pedophilia*. https://doi.org/10.1007/978-3-319-45510-5_61

Viscusi, G., Collins, A., & Florin, M. V. (2020). Governments' strategic stance toward artificial intelligence: An interpretive display on Europe [Paper presentation]. ACM International Conference Proceeding Series in ICEGOV '20. New York, NY, USA: Association for Computing Machinery (pp. 44–53). https://doi.org/10.1145/3428502.3428508

Wang, J., Hwang, G.-H., & Chang, C.-Y. (2021). Directions of the 100 most cited chatbot-related human behavior research: A review of academic publications. *Computers and Education: Artificial Intelligence*, *2*, 100023. https://doi.org/10.1016/j.caeai.2021.100023

Web Accessibility Initiative Group (2023). *Web Content Accessibility Guidelines (WCAG 2.2).* https://www.w3.org/TR/WCAG22/

Weisburd, D. L., & McEwen, T. (2015). Introduction: Crime mapping and crime prevention. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2629850

Wilson, L., & Marasoiu, M. (2022). The development and use of Chatbots in public health: scoping review. *JMIR Human Factors*, *9*(4), e35882. Oct. https://doi.org/10.2196/35882

World Wide Web Consortium (W3C). (2021). *Preliminary insights from a Chatbot accessibility playbook and wizard-of-Oz study - submission for the WAI-CooP project and the W3C APA symposium on research and development questions in digital accessibility.* [Online]. https://www.w3.org/WAI/about/projects/wai-coop/paper107.html

World Wide Web Consortium (W3C). (n.d.a). *Web Content Accessibility Guidelines (WCAG) 2.1.* [Online]. https://www.w3.org/TR/WCAG21/

World Wide Web Consortium (W3C). (n.d.b). *User Agent Accessibility Guidelines (UAAG) Overview | Web Accessibility Initiative (WAI) | W3C.* [Online]. https://www.w3.org/WAI/standards-guidelines/uaag/

Yoo, J., & Cho, Y. (2022). ICSA: Intelligent chatbot security assistant using Text-CNN and multi-phase real-time defense against SNS phishing attacks. *Expert Systems with Applications*, *207*, 117893. https://doi.org/10.1016/j.eswa.2022.117893

Zambrano, P., Sanchez, M., Torres, J., & Fuertes, W. (2017). *BotHook: An option against Cyberpedophilia* [Paper presentation]. 2017 1st Cyber Security in Networking Conference, CSNet 2017 (pp. 1–3). https://doi.org/10.1109/CSNET.2017.8241994

Zuiderwijk, A., Chen, Y.-C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Gov Inf Q*, *38*(3), 101577. https://doi.org/10.1016/j.giq.2021.101577

About the authors

Luis Pimentel holds a PhD in Web Science from UTAD and researches cybercrime awareness, AI tools, and digital safety. He is a Portuguese Judicial Police inspector with 30 years of experience in cybercrime and international cooperation. Additionally, he speaks publicly to promote knowledge and prevention in the digital realm of security.

Maria do Rosário Bernardo holds a PhD in Management from the University of Lisbon and has taught Economics, Management, and Information Systems at Universidade Aberta since 1997. Her research focuses on decision-making, management information systems, and e-government and has resulted in numerous publications in these fields.

Tânia Rocha is a researcher at INESC TEC and Assistant Professor at UTAD, specializing in Human-Computer Interaction (HCI). With a background in Multimedia, her research advances User Interface and User Experience (UI/UX) design, fostering user-centred innovation in health, education, and technology, and addressing the needs of diverse and underrepresented communities.