O papel dos chatbots no governo eletrónico

A consciencialização para a criminalidade informática em Portugal

The role of chatbots in e-government

The awareness of computer crime in Portugal

Luis Pimentel [1,2,4], Maria do Rosário Matos Bernardo[2,5], Tânia Rocha[1,3,6]
[1]*Universidade de Trás-os-Montes e Alto Douro*, Vila Real, Portugal
[2]*CEG-Universidade Aberta*, Portugal
[3]*INESC-TEC, Polo de Vila Real*, Vila Real, Portugal
[4]al75334@alunos.utad.pt, [5]maria.bernardo@uab.pt e [6]trocha@utad.pt

Resumo - **A utilização intensiva de equipamentos eletrónicos e a crescente oferta de serviços pela internet potenciaram a incidência da criminalidade informática. Apesar de existirem, em Portugal, medidas públicas que visam promover as competências digitais dos cidadãos em questões de segurança e privacidade de equipamentos eletrónicos, acabam por não ser vocacionadas para aspetos mais complexos deste género de criminalidade. Devido a esta especificidade, medidas preventivas do fenómeno podem beneficiar com o *know-how* e experiência de entidades com competências legais na área, mormente o *Centro Nacional de Cibersegurança (CNCS)*, o *Ministério Público (MP)* e a *Polícia Judiciária (PJ).* Na administração pública, em Portugal, verifica-se a adoção de tecnologias emergentes, baseadas em inteligência artificial (IA), para potenciar a comunicação entre Estado e cidadãos. Ações de sensibilização abrangentes devem socorrer-se destas ferramentas tecnológicas. Deste modo, este artigo descreve a investigação conducente à identificação de uma ferramenta eletrónica (artefacto) eficiente, em contexto de governo eletrónico, com o objetivo de informar e consciencializar os cidadãos para o crescente fenómeno da criminalidade informática.**

Palavras Chave - acessibilidade; chatbot; criminalidade informática; ética; governo eletrónico; privacidade.

Abstract – **The intensive use of electronic equipment and the growing offer of services over the Internet has increased the incidence of computer crime. Although there are public measures in Portugal aimed at promoting the digital skills of citizens in matters of security and privacy of electronic equipment, they need to address the more complex aspects of this type of crime. Due to this specificity, preventive measures of the phenomenon may benefit from the know-how and experience of entities with legal powers in the area, especially the National Center for Cybersecurity (CNCS), the Public Prosecutor's Office (MP), and the Judicial Police (PJ). In the public administration in Portugal, emerging technologies based on artificial intelligence (AI) are being adopted to enhance communication between the State and citizens. Awareness-raising extensive actions should make use of these technological tools. Thus, this article describes the research leading to the identification of an efficient electronic device (artifact) in an e-government context aimed at informing and raising awareness among citizens about the growing phenomenon of cybercrime.**

Keywords - accessibility; chatbot; computer crime; ethics; e-government; privacy.

I. INTRODUÇÃO

O manuseamento de equipamentos eletrónicos para múltiplas finalidades, bem como a oferta intensiva de serviços presentes em plataformas de internet, possibilitaram que os fenómenos de criminalidade informática tivessem um incremento significativo nos últimos anos [1], [2]. Através de simples ações ou esquemas mais complexos, os perigos cibernéticos fazem parte do quotidiano dos utilizadores [3], [4]. Situações mais complexas podem comprometer a segurança dos utilizadores e respetivos equipamentos eletrónicos [5]. A consciencialização para este problema pode contribuir para adequar comportamentos, evitando-se assim a vitimização [4], [6]. Se o pensamento critico ou análise cuidada de conteúdos pode superar alguns desafios intelectuais, a perceção de uma grande parte dos crimes informáticos revela-se mais complexa. Segundo o Relatório Cibersegurança em Portugal – Sociedade 2020 [7], do CNCS, a educação e a sensibilização para os fenómenos de cibersegurança são uns dos pilares para sua prevenção. Revestem-se da capacidade de influenciar atitudes e mudar os comportamentos perante o fenómeno [7]. Importa, deste modo, conceber formas adequadas de prevenção quanto às múltiplas ações e tipologias da criminalidade informática, incluindo, neste processo, entidades públicas credenciadas para o efeito.

Como ponto de partida da investigação, formulou-se a questão *"Que tipo de solução informática (artefacto) poderá ser idealizada para promover competências digitais e prevenir a criminalidade em Portugal?"*. Os objetivos passaram por: (1) identificar características da criminalidade informática, nomeadamente quanto às vitimas e entidades responsáveis pela sua mitigação, (2) identificar as medidas, em contexto de governo eletrónico, promotoras de competências digitais, mormente para a prevenção da criminalidade informática, (3) estudar diferentes tipos de ferramentas (artefactos) com potencialidade para a prevenção da criminalidade informática, (4) definição de um projeto para a idealização de um artefacto, com observância de atributos de acessibilidade, usabilidade e experiência do utilizador (UX), na perspetiva de vir a ser implementado, futuramente, na administração pública.

2023 18th Iberian Conference on Information Systems and Technologies (CISTI)
20 – 23 June 2023, Aveiro, Portugal
ISBN: 978-989-33-4792-8

A metodologia da investigação baseou-se, inicialmente, de forma preliminar, em pesquisas exploratórias sobre as tecnologias e ferramentas com maior potencial, em contexto de governo eletrónico, para promover, de forma eficiente, a comunicação entre o estado e os cidadãos. A IA, como tecnologia, e os chatbots, como ferramenta, acabaram por se destacar neste processo. Com maior objetividade, através de metodologia de revisão sistemática da literatura, com recurso às bibliotecas digitais ACM Digital Library, IEEE Digital Library, Science Direct, Scopus, e Web of Science, foram extraídos e analisados dados conducentes a objetivos específicos: (1) a identificação das áreas de implementação dos chatbots, nomeadamente em contexto de governo eletrónico e respetivos atributos, (2) identificação de chatbots em áreas da conciliação da criminalidade informática, mesmo que não se enquadrem no conceito de governo eletrónico, (3) identificação de diplomas legais e diretrizes, em Portugal e nos órgãos legislativos da União Europeia, sobre tecnologias emergentes em contexto de governo eletrónico, (4) identificação de normas e diretrizes de desenvolvimento Web, mormente para chatbots, em contexto do governo eletrónico, em questões de acessibilidade, usabilidade e UX, (5) apuramento de questões de investigação atualmente em aberto, na área de implementação de chatbots em contexto de governo eletrónico, para a consciencialização da criminalidade informática. Os resultados desta pesquisa, a refletir num documento de Revisão Sistemática de Literatura (RSL) atualmente em relatório, apontam os chatbots como uma ferramenta adequada ao propósito investigado.

O presente artigo encontra-se dividido em seis secções: a secção II faz referência à criminalidade informática e respetiva caracterização, seja ao nível das suas vítimas, como das entidades públicas responsáveis pela sua mitigação, a secção III aborda as medidas governamentais que visam o incremento das competências digitais, as tecnologias e ferramentas que integram a administração pública, respetivamente a IA e os chatbots, bem como questões de ética, a secção IV diz respeito a técnicas e práticas de desenvolvimento Web relativos a fatores de acessibilidade, usabilidade e UX, a secção V descreve e caracteriza os chatbots, mormente no plano do governo eletrónico, com alusão a questões de privacidade, proteção de dados, bem como possíveis estratégias de prevenção da criminalidade informática, na secção VI descreve-se a proposta de arquitetura baseada em chatbots, a secção VII, reflete as conclusões da investigação.

II. A CRIMINALIDADE INFORMÁTICA

Atualmente, assiste-se a um aumento significativo da criminalidade informática [1], [2] e respetivas vítimas, de todas as idades, condições sociais ou académicas, com maior incidência na pandemia COVID-19 [8]. A criminalidade informática diz respeito às atividades delituosas que envolvem computadores, sistemas informáticos e outros dispositivos eletrónicos, ligados em rede ou à internet, seja como instrumento ou como alvo desses mesmos crimes [9]. Abrange os delitos da *Lei do Cibercrime* [10], respeitante a crimes cibernéticos, bem como delitos cometidos com recurso a meios informáticos, previstos, em grande parte, no *Código Penal* [11].

A. O incremento da criminalidade informática

O Relatório Cibersegurança em Portugal, Riscos e Conflitos 2022 [2], do CNCS, reflete uma grande incidência do cibercrime. Estes números dizem apenas respeito aos dados reportados ao CNCS e recolha de dados junto de outas entidades, não correspondendo, assim, à sua verdadeira dimensão [2]. De igual forma, o *Relatório Anual de Segurança Interna de 2021 (RASI)* [1], elaborado pelo *Sistema de Segurança Interna (SSI)*, também reflete o aumento da criminalidade. Estas estatísticas dizem respeito às incidências do cibercrime, não sendo assim contabilizados os crimes ciberdependentes, isto é, delitos cometidos com recurso a meios informáticos, como é o caso do abuso sexual de crianças, cyberbullying, fraudes bancárias, fraudes com cartões bancários, branqueamento de capitais, extorsão ou burlas informáticas [1].

B. Incidência da criminalidade informática

Esquemas fraudulentos sofisticados dificultam a proteção de vítimas e dispositivos eletrónicos, no entanto, existem situações que podem ser prevenidas, como é o caso de simples distrações.

1) A vulnerabilidade das vítimas: a diversidade do crime informático leva a que alguns utilizadores desconheçam a nova realidade, tornando-se fundamental promover a sua literacia digital da área. Estes crimes atingem utilizadores incautos e mais vulneráveis, desconhecedores dos modos de atuação criminal, bem como de normas básicas de segurança. A população mais vulnerável diz respeito a pessoas de idade mais avançada [12], com eventuais formas de incapacidade, sejam elas motoras ou cognitivas [13], podendo ser vítimas de: (1) fraudes financeiras, (2) fraudes no namoro, (3) fraudes no comércio eletrónico, (4) branqueamento de capitais (*money mule*), (5) e *phishing*, seja por e-mail, SMS ou redes socais.

2) A vulnerabilidade emocional das algumas vítimas: esta vulnerabilidade manifesta-se em algumas atuações, como é o caso da fraude *romance scam* (fraude no namoro) [14]. Atendendo ao estigma social decorrente de perdas financeiras avultadas, as vítimas acabam por revelar sentimentos de culpa e vergonha [14]. Este facto acaba por inibir eventuais pedidos de ajuda às autoridades e familiares. Os atributos de anonimato e reserva dos chatbot podem favorecer, neste caso, a recolha de informação pertinente por parte das vítimas.

C. Entidades públicas e criminalidade informática

As entidades responsáveis por políticas de cibersegurança do Estado ou investigação da criminalidade informática, respetivamente, o CNCS [15], MP [16] e a PJ [17], atendendo aos seu know-how e experiência, devem participar em eventuais medidas de sensibilização, promovidas em contexto de governo eletrónico.

III. O GOVERNO ELETRÓNICO

A importância dos ambientes tecnológicos, nomeadamente em questões de segurança informática, levou ao surgimento de iniciativas estratégicas, em contexto de governo eletrónico, para o incremento das competências digitais [18], [19].

A. Medidas de incremento das competências digitais

1) A Iniciativa Nacional de Competências Digitais e.2030, Portugal (INCoDe.2030)[18] refere-se à necessidade de

2023 18th Iberian Conference on Information Systems and Technologies (CISTI)
20 – 23 June 2023, Aveiro, Portugal
ISBN: 978-989-33-4792-8

incremento das competências nas novas tecnologias digitais. Esta medida pretende "responder às carências diagnosticadas nas competências digitais dos portugueses, com vista a Portugal se posicionar na vanguarda europeia até 2030", bem como "incentivar à qualificação e especialização digital da população ativa, empregada e desempregada" [18].

2) O Quadro Dinâmico de Referência de Competência Digital: é caracterizado como fundamental para o sucesso do *INCoDe.2030*, que levou à criação deste *Quadro Dinâmico de Referência de Competência Digital (QDRCD)* [19], com vista à adoção do *Quadro Europeu de Competência Digital para Cidadãos (DigComp 2.1)*, relativo "a conceitos, níveis de complexidade e autonomia dos utilizadores, em contexto de competências digitais". Neste quadro, encontram-se mencionadas cinco áreas que agregam as diversas competências digitais que importa promover: (1) a literacia da informação, (2) a comunicação e cidadania, (3) a criação de conteúdos, (4) a segurança e privacidade, (5) e o desenvolvimento de soluções. Muito embora as competências digitais para enfrentar a criminalidade informática não sejam diretamente focadas, o QDRCD refere-se à necessidade de implementação de medidas que promovam competências digitais em áreas da segurança e privacidade, nomeadamente quanto à proteção de dispositivos, conteúdos digitais e dados pessoais [19].

B. A inteligência artificial em contexto de governo eletrónico

As entidades governamentais têm demonstrado interesse em tecnologias baseadas em IA para melhorar os serviços públicos. Contudo, apesar das vantagens apresentadas por decisores políticos, desconhece-se o seu real impacto no sector [20].

1) As questões de Ética na IA: refletem-se em diversas áreas, como é caso dos direitos do Homem, da privacidade, da segurança e proteção de dados, devendo, por esse motivo, serem contempladas em decisões políticas [21]. Ao nível europeu, entre outros, verifica-se a existência da *European Framework on Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies* [22] "relativa à proteção de princípios éticos, na implantação e utilização de IA, robótica e tecnologias relacionadas, em interações com humanos" [22].

2) Sobre questões de Ética e chatbots: importa mencionar que os chatbots, no domínio de interação com cidadãos, representam uma grande maioria de utilização da AI [20], levando a que estas preocupações acabem por se refletir, de forma pronunciada, neste âmbito [20], [23].

IV. ACESSIBILIDADE, USABILIDADE E UX

As práticas de desenvolvimento Web passam por considerar fatores de acessibilidade, usabilidade e UX. Estes conceitos concorrem para a criação de uma teia cujo principal objetivo é a criação de um ambiente Web que sirva o seu propósito e as pretensões de todos os utilizadores [24]. O desenvolvimento Web, considerando estes fatores, aponta para a implementação de técnicas inovadoras, como é o caso das propostas nas áreas de arquitetura de software baseadas em agentes inteligentes [25].

A. Acessibilidade

Para o *World Wide Web Consortium (W3C)* [24], a acessibilidade permite "que as pessoas com deficiência possam perceber, compreender, navegar, interagir com a Web e contribuir para a mesma". Promove a UX, mesmo em casos de alguma deficiência. Potencia a perceção, compreensão, navegabilidade e a interação, através dos conteúdos [26].

Em Portugal, a administração pública segue regras rigorosas de acessibilidade em sítios Web, previstas no *Decreto-Lei n.º 83/2018, de 19 de outubro* [27], respeitante à transposição da *Diretiva (EU) 2016/2102* [28], relativa à mesma matéria.

B. Usabilidade

A usabilidade foca-se em produtos eficazes, eficientes e satisfatórios, tendo em vista a UX [29] . Focam-se aspetos que possam incluir utilizadores com eventuais deficiências. A acessibilidade e usabilidade possuem um papel fulcral em UX. Torna-se necessário conhecer e caracterizar os utilizadores, centrando-se a ação nas suas pretensões, prevendo as suas necessidades, bem como avaliar a sua literacia digital [29].

C. Experiência do utilizador (UX)

Tendo em conta fatores de UX, pretende-se a qualidade da interação do utilizador com um produto ou serviço, através de conteúdos úteis e páginas acessíveis a todos os utilizadores [30]. Pesquisa-se sobre preferências, layouts, bem como a concreta implementação de usabilidade [29] e acessibilidade [30].

D. Guias e práticas de desenvolvimento

Os conceitos de acessibilidade, usabilidade e UX encontram-se associados a diversos guias e práticas de desenvolvimento Web: (1) *Accessibility, Usability, and Inclusion* [24], (2) *Introduction to Web Accessibility* [26], (3) *Web Content Accessibility Guidelines (WCAG) 2.1* [31], (4) *User Agent Accessibility Guidelines (UAAG) Overview* [32] , (5) e *Essential Components of Web Accessibility* [33].

E. Técnicas de avalização

Esta etapa permite aferir o desempenho e conceção de projetos, através de diversos métodos e ferramentas, visando aferir fatores de acessibilidade e usabilidade. Os testes podem ser realizados através de métodos assentes na análise de peritos (análise cognitiva, avaliação heurística, modelos ou estudos), bem como pela participação de outros utilizadores menos experientes, seja em ambiente de laboratório ou pesquisas de campo, nomeadamente com recurso a inquéritos [34].

1) No campo das heurísticas: Nielson [35] refere-se a dez regras gerais. Estes aspetos encontram-se relacionados com: (1) visibilidade do status do sistema, (2) correspondência entre o sistema e o mundo real, (3) controlo e liberdade do utilizador, (4) consistência e padrões, (5) prevenção de erros, (6) reconhecimento em vez de recordação, (7) flexibilidade e eficiência, (8) estética e design minimalista, (9) reconhecer, diagnosticar e resolver erros, (10) bem como ajuda e documentação [35].

2) Sobre as ferramentas para avaliação de acessibilidade: entre outros, podemos fazer referência ao *acessMotitor 2.1* [36], da *Agência para a Modernização Administrativa (AMA)*. Através de um URL ou código HTML, é avaliada e validada a conformidade relativa às boas práticas de acessibilidade Web *(WCAG 2.1 do W3C).*

2023 18th Iberian Conference on Information Systems and Technologies (CISTI)
20 – 23 June 2023, Aveiro, Portugal
ISBN: 978-989-33-4792-8

3) Sobre ferramentas para avaliação de usabilidade: o *System Usability Scale (SUS)* [37], [38], de uma forma confiável e rápida, mede fatores de usabilidade (efetividade, eficiência e satisfação), através de um questionário de 10 itens, com respeito pelas heurísticas de Nielsen [35].

4) Sobre experiência do utilizador em dispositivos móveis: a ferramenta *Google Mobile-Friendly Test* [39] permite avaliar a conformidade de uma página *Web*, quando utilizada em dispositivos móveis.

V. OS CHATBOTS

No decorrer da investigação preliminar da literatura, pelas características evidenciadas, os chatbots surgiram como uma ferramenta tecnológica apropriada, para, de forma eficiente, contribuir para a prevenção da criminalidade informática.

A. Atributos gerais dos chatbots

Os chatbots são caracterizados como sistemas de software inteligentes que podem manter uma conversação com humanos, seja por texto ou voz, usando linguagem natural, em tempo real [40]. As suas vantagens passam por [41]: (1) facilidade de interação, (2) rapidez de reação, (3) uniformização e universalidade da informação, (3) capacidade de configuração, (4) interação por texto ou voz, (5) complementaridade de sistemas informáticos com processos de análise, (6) facilidade e simplicidade de interação, (7) rapidez de reação, (8) uniformização e universalidade da informação, (9) múltipla capacidade de configuração; (10) e plena disponibilidade de temporal (24 horas por dia/ sete dias por semana).

B. Chatbots em contexto de governo eletrónico

A transformação digital levou a encarar os chatbots como uma tecnologia em destaque, bem como um meio adequado de promover a comunicação entre Estado e cidadãos, em diversas áreas da administração pública [42]. Em Portugal assiste-se ao interesse por tecnologias baseadas em AI e chatbots, refletido em medidas previstas no *Simplex* [43]. Para processos de atendimento, observam-se chatbots nos sítios *Web da Direção-Geral das Atividades Económicas (DGAE)*[1] e *Direção Geral do Consumidor (DGC)*[2]. Segundo os seus responsáveis, "esta ferramenta é um excelente ponto de partida da utilização de modelos de inovação baseados em IA, permitindo simplificar o trabalho da Administração Pública" [43]. Verificam-se ainda chatbots em sítios Web de diversas autarquias[3] (Lisboa, Murça, Vimioso e Mirandela).

Os chatbots constituem um conceito inovador e por explorar na administração pública [44], sendo que os sítios Web do CNCS[4], do MP [5] e PJ[6] não possuem esta ferramenta.

C. Atributos dos chatbots em contexto de governo eletrónico

Neste contexto, estudos recentes [42], [45]–[47], referem-se a alguns atributos dos chatbots: (1) possibilitam a inovação tecnológica [46], (2) promovem a IA [47], (3) impulsionam a comunicação [47], (4) incrementam as competências sociais [45], (5) aumentam a interação [42], [45], (6) revestem-se de autenticidade [47], (7) possuem um grande potencial[46], (8) são versáteis [42], (9) e possuem múltipla aplicabilidade [47].

D. Privacidade e proteção de dados

Os chatbots, através de técnicas de aprendizagem automática, recolhem dados pessoais dos utilizadores pra diversos fins [48]. Na União Europeia (EU) observe-se o *Regulamento (UE) 2016/679* [49] "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais" [49]. o *Regulamento Geral de Proteção de Dados (RGPD)* também se aplica a Portugal [50], [51]. No caso dos chatbots, a pretensão de acesso a dados pessoais, carece de autorização ao abrigo deste regulamento [48]. Algumas das preocupações identificadas sobre estas preocupações passam por [48]: (1) utilização de cookies, (2) dados resultantes da interação, (3) e dados de identificação do utilizador (e-mail, nome e ID de dispositivos).

E. Os chatbots na prevenção da criminalidade informática

Muito embora o envolvimento de entidades responsáveis pela mitigação da criminalidade informática, em contexto de governo eletrónico, não seja explorado, chatbots são mencionados em algumas soluções de cibersegurança: (1) em aspetos generalistas do fenómeno [52], (2) no cyberbullying [53], (3) na recolha de dados na *dark* Web [54], (4) na formação de ciberanalistas [55], (5) na prevenção de ações de engenharia social [56], (6) e cibersegurança no contexto escolar [55]. Os chatbots, ao permitem massificar a transmissão de conhecimento [57], podem, deste modo, desempenhar um papel de relevo, em contexto de governo eletrónico, na mitigação da criminalidade informática.

VI. ARQUITETURA PROPOSTA

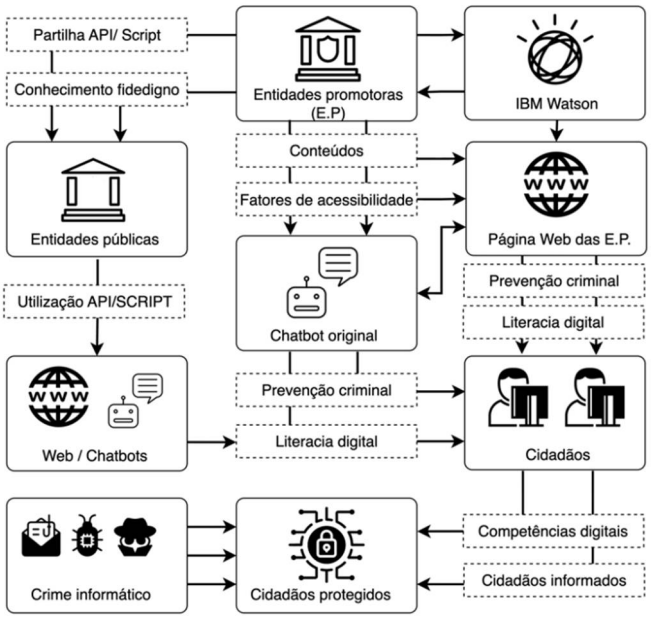

Figura 1. Diagrama da arquitetura proposta, baseada em chatbots.

[1] https://www.dgae.gov.pt
[2] https://www.consumidor.gov.pt
[3] https://www.lisboa.pt; https://www.cm-murca.pt; https://www.cm-vimioso.pt; https://www.cm-mirandela.pt
[4] https://www.cncs.gov.pt
[5] https://cibercrime.ministeriopublico.pt; https://www.ministeriopublico.pt
[6] https://www.policiajudiciaria.pt

ISBN: 978-989-33-4792-8

A arquitetura proposta assenta essencialmente em conhecimentos técnicos sobre o tema, bem como na experiência profissional do primeiro autor, enquanto investigador da Polícia Judiciária, na área da criminalidade informática. Apesar deste facto, importa proceder-se à sua validação científica, a implementar em fases posteriores do projeto de investigação doutoral. A arquitetura idealizada foca-se na utilização de chatbots em sítios Web governamentais, implementados e geridos por equipas conjuntas do CNCS, MP e PJ. Não obstante a possível identificação de outros recursos avançados em investigações futuras, a título exemplificativo, o IBM Watson permite a partilha de recurso por *API* ou *Srcipt*, possibilitando a multiplicação destes agentes conversacionais junto de outras entidades públicas.

A. *Plataformas de desenvolvimento e implantação de chatbots*

Verificam-se diversas plataformas com recursos para a implementação e gestão de chatbots, seja o *IBM Watson Assistant, o Amazon Lex, o Amazon Polly, o Dialogflow ou o Amelia Nuance* [58]. Apesar do conhecimento sobre a plataforma do *IBM Watson Assistant* por parte do primeiro autor, importar proceder-se a um estudo específico, atualmente em estruturação, para identificação de ferramentas e tecnologias de desenvolvimento de chatbots, com alusão aos respetivos requisitos de software e poder computacional.

B. *Layouts promotores de acessibilidade*

Fatores de acessibilidade, usabilidade e UX, também devem ser considerados em qualquer projeto tecnológico [53]. Entre outros aspetos a implementar, a idealização de layouts mistos, com a introdução de uma interface de pesquisa por texto ou simples visualização, poderá constituir uma ajuda preciosa para utilizadores que apresentem eventuais dificuldades de escrita. Nesse sentido, árvores de decisão, devidamente estruturadas, com recurso a campos de texto, podem também favorecer a navegação por toque (dispositivos móveis) ou clique de rato (outros equipamentos informáticos).

VII. CONCLUSÕES

A massificação de utilização de recursos tecnológicos levou a um incremento significativo da criminalidade informática. Apesar de existirem, em Portugal, medidas públicas que visam a promoção de competências digitais, não são especificas para este este fenómeno. A complexidade destes fenómenos carece do envolvimento de entidades credenciadas na área (CNCS, MP e PJ), com vista credibilizar ações de mitigação. Os atributos chatbots e conceitos de desenvolvimento Web, tendo em conta fatores de acessibilidade, usabilidade e UX, fazem desta ferramenta uma opção a considerar para a idealização de um artefacto adequada. A arquitetura agora proposta, embora careça de validação no âmbito da investigação de doutoramento em curso, pretende garantir elevados índices de estabilidade, escalabilidade e resiliência de recursos. Pretende-se ainda que venha a ser garantida a réplica de chatbots, seja por *API* ou *Script*. A introdução mista de layouts, seja por etiquetas de texto ou campo de escrita, possibilita ainda utilização destes chatbots por parte de utilizadores que eventualmente possuam dificuldades na escrita. O caráter não lucrativo do artefacto torna desnecessária a recolha de dados pessoais ou a monitorização das atividades dos utilizadores, ultrapassando-se, dessa forma, algumas das questões de ética, privacidade e proteção de dados. Tendo em conta que se trata de uma área por explorar e com grande potencial, julga-se pertinente um estudo aprofundado sobre a idealização e possível implementação de chatbot em sítios Web da administração pública, com o envolvimento de equipas do CNCS, MP e PJ, para consciencializar os cidadãos face os crescentes perigos da criminalidade informática.

Os resultados expostos no presente artigo constituem uma base de partida para trabalhos futuros, a desenvolver na investigação de doutoramento, tendo em conta o diagrama da Figura 1 e com o enquadramento metodológico Design Science Research (DSR), para atingir os seguintes objetivos:: (1) determinar o estado atual de idealização e implantação de chatbots na administração pública em Portugal, (2) estudar as condições técnicas do desenvolvimento, desempenho, funcionalidades e ambientes de implantação dos chatbots, (3) estudar os atributos dos chatbot com foco na acessibilidade, usabilidade e UX (4) identificar formas de testar e validar o artefacto, (5) em que moldes pode ser proposta a integração deste artefacto em ecossistemas da administração pública em Portugal, com observância de todos os aspetos legais.

REFERÊNCIAS BIBLIOGRÁFICA

[1] SSI, «Relatório Anual de Segurança Interna (RASI - 2021)», 2022.

[2] CNCS, «Relatório Cibersegurança em Portugal – Riscos e Conflitos - 3a Edição.», 2022.

[3] K. Singh, «Increment of Cyber Crimes against Our Securities», vol. 12, n. April, pp. 116–120, 2011.

[4] D. L. Weisburd e T. McEwen, «Introduction: Crime Mapping and Crime Prevention», SSRN Electronic Journal, 2015, doi: 10.2139/ssrn.2629850.

[5] L. F. Tatarinova, K. N. Shakirov, e D. v Tatarinov, «Criminological analysis of determinants of cybercrime technologies», Mathematics Education, vol. 11, n. 5, pp. 1127–1134, 2016.

[6] S. Srivastava, K. Srivastava, e N. Arora, «Exploration of a Solution-Centric Crime Awareness Tool», Int J Comput Appl, vol. 175, n. 22, pp. 26–32, 2020, doi: 10.5120/ijca2020920743.

[7] CNCS, «Relatório Sociedade 2020», 2020. https://www.cncs.gov.pt/pt/relatorio-sociedade-2020/ (acedido Jan. 22, 2023).

[8] S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C. Whybrow, e T. Glenn, «Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry», Curr Psychiatry Rep, vol. 23, n. 4, 2021, doi: 10.1007/s11920-021-01228-w.

[9] E. Peternwaike e D. P. Criminology, «A systematic literature review on criminological research on the history of cybercrime focusing on type of crime and geographic origin of the perpetrators», n. August, 2021.

[10] Assembleia da República, «Lei no 109/2009, de 15 de Setembro (Lei Cibercrime)», Diário da República n.o 165/2008, Série I de 2008-08-27, pp. 6038–6042, 2009.

[11] Assembleia da República, «Decreto-Lei n.o 48/95, 15 de Março (Código Penal)», Diário da República n.o 63/1995, Série I-A de 1995-03-15, 1995.

[12] A. Kalache e A. Gatti, «Active ageing: a policy framework.», Advances in gerontology = Uspekhi gerontologii / Rossiiskaia akademiia nauk, Gerontologicheskoe obshchestvo, vol. 11, pp. 7–18, 2003, doi: 10.1080/tam.5.1.1.37.

[13] Agência para a Modernização Administrativa, «Página Inicial - acessibilidade.gov.pt», 2021. https://www.acessibilidade.gov.pt/ (acedido Jan. 22, 2023).

[14] P. Anesa, «Lovextortion: Persuasion strategies in romance cybercrime», Discourse, Context & Media, vol. 35, p. 100398, 2020, doi: https://doi.org/10.1016/j.dcm.2020.100398.

[15] Presidência do Conselho de Ministros, «Decreto-Lei no 3/2012, de 16 de Janeiro (Orgânica CNCS)», Diário da República n.o 11/2012, Série I de 2012-01-16, pp. 174–177, 2012.

ISBN: 978-989-33-4792-8

[16] PGR, «Procuradoria-geral da república - Despacho de criação Gabinete Cibercrime, de 7 de dezembro de 2011.» 2011.

[17] Assembleia da República, «Lei 49/2008, de 27 de agosto (LOIC)», Diário da República n.o 165/2008, Série I de 2008-08-27, pp. 6038–6042, 2008.

[18] Presidência do Conselho de Ministros, «Resolução do Conselho de Ministros n.o 26/2018, de 8 de março (INCoDe.2030)», : Diário da República n.o 48/2018, Série I de 2018-03-08, pp. 1207–1209, 2018.

[19] Presidência do Conselho de Ministros, «Despacho n.o 1088/2019, de 31 de janeiro (QDRCD-DigCom 2.1)», Diário da República n.o 22/2019, Série II de 2019-01-31, pp. 4184–4186, 2019.

[20] A. Zuiderwijk, Y.-C. Chen, e F. Salem, «Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda», Gov Inf Q, vol. 38, n. 3, p. 101577, 2021, doi: https://doi.org/10.1016/j.giq.2021.101577.

[21] D. Susar e V. Aquaro, «Artificial intelligence: Opportunities and challenges for the public sector», em ACM International Conference Proceeding Series, 2019, vol. Part F1481, pp. 418–426. doi: 10.1145/3326365.3326420.

[22] E. Union, European Framework on Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies, n. 9. 2020.

[23] J. Bang, S. Kim, J. W. Nam, e D. G. Yang, «Ethical Chatbot Design for Reducing Negative Effects of Biased Data and Unethical Conversations», em 2021 International Conference on Platform Technology and Service, PlatCon 2021 - Proceedings, 2021. doi: 10.1109/PlatCon53246.2021.9680760.

[24] W3C, «Accessibility, Usability, and Inclusion», 2010. https://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/ (acedido Jan. 12, 2023).

[25] E. Hatsue, M. Huzita, H. Marci, D. Oliveira, e J. Marcos, «Uma proposta de arquitetura de software baseada em agentes. A proposal of agent-based software architecture», Acta Scientiarum - Technology, vol. 22, n. 5, pp. 1339–1346, 2000, doi: 10.4025/actascitechnol.v22i0.3131.

[26] C. F. D. S. Sampaio, «Introduction to web accessibility», New Research on Assistive Technologies: Uses and Limitations, pp. 59–66, 2014.

[27] Presidência do Conselho de Ministros, «Decreto-Lei n.o 83/2018, de 19 de outubro (Acessibilidade sítios Web)», Diário da República n.o 202/2018, Série I de 2018-10-19, pp. 5029–5035, 2018.

[28] Parlamento Europeu e do Conselho da União Europeia, «DIRETIVA (UE) 2016/2102 (acessibilidade dos sítios web)», Jornal Oficial da União Europeia, vol. 2014, n. 2, pp. 1–15, 2016.

[29] Usability.gov, «Usability Evaluation Basics», 2020. https://www.usability.gov/what-and-why/usability-evaluation.html (acedido Jan. 22, 2023).

[30] Usability.gov, «User Experience Basics», Usability.gov, 2017. https://www.usability.gov/what-and-why/user-experience.html (acedido Jan. 14, 2023).

[31] WC3, «Web Content Accessibility Guidelines (WCAG 2.1)», 2018. https://www.w3.org/TR/WCAG21/ (acedido Jan. 27, 2023).

[32] W3C, «User Agent Accessibility Guidelines (UAAG) Overview», 2016. https://www.w3.org/WAI/standards-guidelines/ (acedido Jan. 19, 2023).

[33] WC3, «Essential Components of Web Accessibility». https://www.w3.org/WAI/fundamentals/ (acedido Jan. 28, 2023).

[34] A. Dix, J. Finlay, G. D. Abowd, e R. Beale, Human-Computer Interaction Ch. 9 Evaluation Techniques. 2004. [Em linha]. Available: www.hcibook.com

[35] J. Nielsen, Usability Engineering. Morgan Kaufmann, 1993.

[36] Agência para a Modernização Administrativa (AMA), «Access Monitor - Versão 2.1», 2021. https://accessmonitor.acessibilidade.gov.pt/ (acedido Jan. 30, 2023).

[37] A. I. Martins, A. F. Rosa, A. Queirós, A. Silva, e N. P. Rocha, «European Portuguese Validation of the System Usability Scale (SUS)», Procedia Comput Sci, vol. 67, pp. 293–300, 2015, doi: https://doi.org/10.1016/j.procs.2015.09.273.

[38] Usability.gov, «System Usability Scale (SUS) | Usability.gov». 2020. [Em linha]. Available: https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

[39] Google, «Teste de compatibilidade com dispositivos móveis». https://search.google.com/test/mobile-friendly (acedido Jan. 15, 2023).

[40] P. Suta, X. Lan, B. Wu, P. Mongkolnam, e J. H. Chan, «An overview of machine learning in chatbots», International Journal of Mechanical Engineering and Robotics Research, vol. 9, n. 4, pp. 502–510, 2020, doi: 10.18178/ijmerr.9.4.502-510.

[41] A. Kateryna, R. Oleksandr, T. Mariia, S. Iryna, K. Evgen, e L. Anastasiia, «Digital literacy development trends in the professional environment», International Journal of Learning, Teaching and Educational Research, vol. 19, n. 7, pp. 55–79, 2020, doi: 10.26803/ijlter.19.7.4.

[42] Kumar e Mukund, «A Review of Select Innovations and Emerging Trends in E-Governance», International Journal of Research in Engineering, Science and Management, vol. 3, n. 8, 2020.

[43] Direção-Geral das Atividades Económicas, «Simplex - Assistente virtual simplifica o atendimento», 2021. https://www.dgae.gov.pt/comunicacao/noticias/assistente-virtual-simplifica-o-atendimento-a-empresas-e-a-consumidores.aspx (acedido Jan. 23, 2023).

[44] R. Dias e M. Gomes, «Do Governo Eletrónico à Governança Digital: Modelos e Estratégias de Governo Transformacional», Ciências e Políticas Públicas / Public Sciences & Policies, vol. 7, n. 1, pp. 93–117, 2021, doi: 10.33167/2184-0644.cpp2021.vviin1/pp.93-117.

[45] A. P. Chaves e M. A. Gerosa, «How Should My Chatbot Interact? A Survey on Social Characteristics in Human–Chatbot Interaction Design», Int J Hum Comput Interact, vol. 37, n. 8, pp. 729–758, 2021, doi: 10.1080/10447318.2020.1841438.

[46] K. K. Nirala, N. K. Singh, e V. S. Purani, A survey on providing customer and public administration based services using AI: chatbot, vol. 81, n. 16. Springer US, 2022. doi: 10.1007/s11042-021-11458-y.

[47] J. Wang, G.-H. Hwang, e C.-Y. Chang, «Directions of the 100 most cited chatbot-related human behavior research: A review of academic publications», Computers and Education: Artificial Intelligence, vol. 2, p. 100023, 2021, doi: https://doi.org/10.1016/j.caeai.2021.100023.

[48] M. Hasal, J. Nowaková, K. A. Saghair, H. Abdulla, V. Snášel, e L. Ogiela, «Chatbots: Security, privacy, data protection, and social aspects», Concurr Comput, vol. 33, n. 19, p. e6426, 2021, doi: https://doi.org/10.1002/cpe.6426.

[49] Parlamento Europeu e do Conselho, «Regulamento (UE) 2016/679», Jornal Oficial da União Europeia, vol. 2014, n. 3, pp. 1–119, 2016.

[50] União Europeia, «Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016», Jornal Oficial da União Europeia, n. L 127, pp. 2–6, 2018.

[51] Assembleia da República, «Lei no 58/2019, de 8 de agosto (RGPD)», Diário da República n.o 151/2019, Série I de 2019-08-08, pp. 3–4, 2019.

[52] S. Hamad e T. Yeferny, «A chatbot for information security», arXiv, vol. 20, n. 4. pp. 287–291, 2020.

[53] V. Vijayakumar, «Intelligent Chatbot Development for Text based Cyberbullying Prevention», vol. 17, n. 1, pp. 73–81, 2021.

[54] M. A. Budiman e M. E. Aminanto, «Use of Intelligence Based Agents to Deal with Cyber Crime», Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences, vol. 5, n. 1, pp. 3679–3685, 2022.

[55] S. Srivastava, K. Srivastava, e N. Arora, «Exploration of a Solution-Centric Crime Awareness Tool», Int J Comput Appl, vol. 975, p. 8887.

[56] B. Banire, D. al Thani, e Y. Yang, «Addressing Cyber Security Accessibility: A Qualitative Study», em 34th British HCI Workshop and Doctoral Consortium 34, 2021, pp. 1–5.

[57] N. Albayrak, A. Ozdemir, e E. Zeydan, «An overview of artificial intelligence based chatbots and an example chatbot application | Yapay Zeka Tabanli Rehber Robotlara Genel Bir Bakis ve Örnek Bir Rehber Robot Uygulamasi», 26th IEEE Signal Processing and Communications Applications Conference, SIU 2018, pp. 1–4, 2018.

[58] E. Adamopoulou e L. Moussiades, «Chatbots: History, technology, and applications», Machine Learning with Applications, vol. 2, n. July, p. 100006, 2020, doi:https://doi.org/10.1016/j.mlwa.2020.100006

ISBN: 978-989-33-4792-8