Instituto Superior de Ciências Policiais e Segurança Interna

Inês Patrícia Oliveira Proença

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXIV Curso de Formação de Oficiais de Polícia

A INTELIGÊNCIA ARTIFICIAL NO COMBATE AO TERRORISMO EM PORTUGAL

ESTUDO EXPLORATÓRIO

Orientador:

PROF.ª DOUTORA RAQUEL DUQUE

Lisboa, 13 de Maio 2022

Instituto Superior de Ciências Policiais e Segurança Interna

Inês Patrícia Oliveira Proença

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXIV Curso de Formação de Oficiais de Polícia

A INTELIGÊNCIA ARTIFICIAL NO COMBATE AO TERRORISMO EM PORTUGAL

ESTUDO EXPLORATÓRIO

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna com vista à obtenção do grau de Mestre em Ciências Policiais, elaborada sob a orientação da Professora Doutora Raquel Duque.

Estabelecimento de Ensino: Instituto Superior de Ciências Policiais e Segurança Interna

Curso: XXXIV CFOP

Orientadora: Professora Doutora Raquel Duque

Título: A inteligência artificial no combate ao terrorismo em Portugal – estudo exploratório

Autor: Inês Patrícia Oliveira Proença

Local de Edição: Lisboa

Data de Edição: Maio de 2022

Ao meu avô

Agradecimentos

A conclusão deste trabalho representa o início de uma nova fase há muito tempo aguardada e desejada. Para a realização deste percurso cheio de desafios, várias foram as pessoas que fizeram parte deste longo caminho.

As minhas primeiras palavras de agradecimento são dirigidas para a minha família, em especial aos meus pais, irmãos e avós. Obrigada por todo o apoio ao longo deste cinco anos, principalmente nos dias mais cinzentos. Por serem um apoio constante e por fazerem com que, toda esta distância que nos separou, parecesse insignificante. Todos os valores que me transmitiram fizeram de mim aquilo que sou hoje.

À Polícia de Segurança Pública e ao Instituto Superior de Ciências Policiais e Segurança Interna, pela oportunidade e formação académica, mas também pelas memórias que levarei comigo no coração.

À minha Orientadora, Professora Doutora Raquel Duque, por ter aceite, desde logo, abraçar comigo esta última etapa com toda a disponibilidade, incentivo, dedicação e partilha de sábios conhecimentos e conselhos.

Ao Subcomissário João Sanheiro pela paciência e conhecimentos transmitidos durante o estágio prático e, em especial, à Subcomissário Maria Vilhena por todas as oportunidades de aprendizagem e confiança disposta em mim que enriqueceram esta minha última caminhada.

À Celeste, ao Francisco e à Bárbara, por me terem acolhido sempre como família e por todo o apoio que me têm dado ao longo deste percurso. Um obrigado não é suficiente para agradecer tudo o que têm feito por mim.

Ao 34.º CFOP, pelos momentos vividos e pelas amizades que levo comigo. Um especial obrigado àqueles que foram o meu porto de abrigo ao longo destes anos, que me deram forças quando tudo parecia difícil e que festejaram as minhas vitórias, tornando assim os meus dias mais felizes. Sei que daqui levo amigos para a vida toda.

Ao Francisco, por ao longo destes anos e principalmente neste ano tão difícil, ter sido o meu grande apoio. Por seres um grande pilar na minha vida, pela paciência e por nunca deixares de acreditar em mim.

Por último, mas não menos importante, uma palavra de agradecimento a todos os que colaboraram sem hesitações nesta investigação. Sem vocês não teria sido possível alcançar tanto conhecimento.

Resumo

É através da utilização de tecnologias que a sociedade muda drasticamente. As vantagens são várias, desde maior facilidade de comunicação, aumento da partilha de conhecimento, possibilidade de os cidadãos estarem em qualquer parte do mundo através de um simples clique, entre outras. No entanto, na criminalidade foi possível verificar algumas mudanças através da adaptação desta às tecnologias e a esta nova realidade. Foi possível verificar algumas mudanças, os alvos tornaram-se diferentes e os *modi operandi* passaram a ser outros. O crime de terrorismo não foi uma exceção. O que antes era tendencialmente feito sobre um grande risco e insegurança é agora feito atrás de um computador ou de um telemóvel – deixam de ser necessárias viagens para investigar determinados alvos, as informações e planeamentos de ataques são feitos *online* através de perfis difíceis de detetar, a propaganda é de fácil acesso tornando a radicalização mais rápida e o recrutamento torna-se mais fácil de desenvolver chegando assim a mais pessoas. É neste contexto de mudança que o presente estudo pretende explorar o papel da tecnologia, em específico, da inteligência artificial para combater o terrorismo. No método foi dada preferência a uma abordagem qualitativa, sendo a recolha de dados realizada através de entrevistas semi-estruturadas, sendo depois realizada uma análise de conteúdo, mais especificamente uma análise categorial. A investigação demonstra que atualmente o uso de inteligência artificial em Portugal é incipiente e que, embora as vantagens de se aplicar a inteligência artificial ao combate ao terrorismo sejam variadas, os desafios são complexos, nomeadamente no que concerne à escassez de meios técnicos, dificuldades para aceder a dados pessoais de suspeitos de terrorismo e entraves legislativos.

Palavras-chave: contraterrorismo; inteligência; inteligência artificial; tecnologia; terrorismo;

Abstract

It is through the use of technology that society changes dramatically. The advantages are many, from easier communication, increased knowledge sharing, the possibility for citizens to be anywhere in the world with a simple click, among others. However, it was possible to verify some changes in criminality by adapting it to the technologies and to this new reality. It was possible to verify some changes, the targets became different and the modi operandi became other. The crime of terrorism was not an exception. What used to be done under great risk and insecurity is now done behind a computer or a cell phone - travelling is no longer necessary to investigate certain targets, information and planning of attacks are done online through profiles that are difficult to detect, propaganda is easily accessible, making radicalization faster, and recruitment becomes easier to develop, thus reaching more people. It is in this context of change that this study aims to explore the role of technology, specifically artificial intelligence, in the combat of terrorism. In the method, preference was given to a qualitative approach, being the data collection carried out through semi-structured interview and subsequently performed a content analysis, more specifically a categorical analysis of the various responses, analyzing them in order to find common and divergent points. The research shows that currently the use of artificial intelligence in Portugal is incipient and that, although the advantages of applying artificial intelligence to combat terrorism are manifold, the challenges are complex, namely regarding the scarcity of technical means, difficulties to access personal data of terrorist suspects, and legislative obstacles.

Keywords: counterterrorism; intelligence; artificial intelligence; technology; terrorism;

Lista de Siglas e Abreviaturas

ADN	Ácido desoxirribonucleico
CCTV	*Closed Circuit Television*
CDC	Convenção sobre os Direitos da Criança
CIA	Central Intelligence Agency
DUDH	Declaração Universal dos Direitos Humanos
EMBERS	*Early Model – Based Event Recognation using Surrogates*
ECTC	*European Counter Terrorism Centre*
EU	Europa
EU IRU	*EU Internet Referral Unit*
EURODAC	*European Asylum Dactyloscopy Database*
EUA	Estados Unidos da América
FOI	*Totalförsvarets Forskningsinstitut*
FSS	Forças e Serviços de Segurança
HUMINT	*Human Intelligence*
IA	Inteligência Artificial
IEEE	*Institute of Electrical and Electronics Engineers*
INTERPOL	*International Criminal Police Organization*
LAPD	*Los Angeles Police Department*
NATO	*North Atlantic Treaty Organization*
NIJ	*National Institute of Justice*
NSA	*National Security Agency*
OCDE	*Organisation for Economic Co-operation and Development*
OCHA	*Office for the Coordination of Humanitarian Affairs*
OMC	Organização Mundial de Comércio
ONU	Organizações das Nações Unidas
PSP	Polícia de Segurança Pública
RASI	Relatório Anual de Segurança Interna
TE-SAT	*EU Terrorism Situation & Trend Report*
TFUE	Tratado sobre o Funcionamento da União Europeia
UE	União Europeia
UNESCO	*United Nations Educational, Scientific and Cultural Organization*
UNHCR	*United Nations High Commissioner for Refugees*
UNICRI	*United Nations Interregional Crime and Justice Research Institute*

Índice

Índice de Tabelas

Índice de Figuras

Introdução

Os atuais conceitos de tempo e de distância, paralelamente ao progresso tecnológico, têm-se vindo a diminuir drasticamente. Krahmann (2007), enumera alguns dos eventos que contribuíram para tal mudança como a Guerra Fria, as inovações tecnológicas e os ataques terroristas de 11 de setembro de 2001. Wulf (2007), acrescenta o impacto da globalização, em que as fronteiras se tornaram fluídas e flexíveis, tornando os mercados cada vez mais liberalizados, contribuindo para um aumento da circulação de pessoas. A humanidade está perante uma revolução tecnológica, tão ou mais importante do que a revolução industrial, a qual Ganor (2021) apelida de "revolução da inteligência artificial". Consequentemente as exigências para garantir a segurança são muito maiores (Krahmann, 2007), assim como as vantagens e benefícios do progresso tecnológico apresentam desafios, nomeadamente no âmbito do combate à criminalidade. Novas tecnologias como a inteligência artificial (IA), aplicações de telemóveis, robótica, veículos autónomos, trazem novos desafios à segurança nacional e internacional conduzindo a novas formas de crime e de alvos (Choo et al., 2007; Rego, 2017). Um dos fenómenos onde tal é observado é no terrorismo que constitui atualmente uma das maiores preocupações das Forças e Serviços de Segurança (FSS) (Martins, 2010).

No relatório da Europol — *EU Terrorism Situation & Trend Report* (TE-SAT) — foi possível verificar que a radicalização e o recrutamento têm vindo a ser uma preocupação crescente, tal como o aumento do consumo de conteúdo extremista despoletado pela pandemia provocada pelo vírus COVID-19. É fácil verificar que o crime de terrorismo soube adaptar-se e retirar vantagens da evolução das tecnologias e comunicações. Consequentemente, a Europa (EU) afirma que, atualmente, um dos maiores desafios securitários é a auto radicalização de jovens unidos por ideologias, conectados através de canais, fóruns e plataformas *online* (Europol, 2021).

O fenómeno terrorista apresenta uma enorme versatilidade onde as táticas e os objetivos são sempre distintos, desenvolvendo-se diferentes métodos ao longo dos tempos (Duque, 2016). Os *lone wolves* são um exemplo dessa mudança, tal como tarefas perigosas que passam agora a ser mais seguras e rápidas. Invariavelmente, a deteção destes ataques torna-se extremamente difícil (Wagner, 2007). Durante a Guerra Fria, os serviços de informações trabalhavam numa estrutura previsível, linear e relativamente simples, atualmente trabalham num ambiente de instabilidade e total imprevisibilidade (Nomikos & Liaropoulos, 2010). É neste clima de insegurança que a IA surge como resposta (Elias & Guedes, 2010).

Atualmente a IA é uma das prioridades da União Europeia (UE), estando a ser desenvolvidos vários regulamentos. De acordo com a Comissão Europeia (2020a), estas ferramentas podem ser oportunidades para proteger os cidadãos dos atos terroristas, através da identificação de propaganda terrorista *online*, de transações suspeitas na venda de produtos

perigosos, de objetos perigosos ocultos ou substâncias ou produtos ilícitos, tal como prestar assistência a cidadãos em emergência e ajudar a guiar equipas de primeira intervenção.

Portugal desenvolve o documento "IA Portugal 2030". Uma estratégia com o objetivo de reunir todos os interessados em construir um mercado de trabalho com a finalidade de usar as novas tecnologias para ajudar a resolver os maiores desafios do mundo e principalmente do setor público (Fundação para a Ciência e Tecnologia, 2021). Portugal é bastante ativo em vários campos de pesquisa nomeadamente em análise de grandes quantidades de dados, *machine learning*[1], sistemas inteligentes, sensoriamento remoto[2], manutenção de infraestruturas críticas e eficiência energética. Embora Portugal seja especialista em áreas como o processamento natural de linguagem[3], tomada de decisão e desenvolvimento de *software* através de IA, o foco continua a ser apenas na educação, saúde, agricultura e indústria, deixando de lado a segurança (Fundação para a Ciência e Tecnologia, 2021).

Desta forma, o presente trabalho de investigação pretende contribuir para o aumento de conhecimento científico sobre a utilização de IA no combate ao terrorismo em Portugal de modo a, por um lado, aumentar a capacidade de prevenção de novos ataques terroristas e, por outro lado, melhorar o aproveitamento dos recursos tecnológicos disponíveis para o cumprimento da missão policial. De forma a alcançar o nosso objetivo, optámos por dividir o trabalho em quatro grandes capítulos, antecedidos pela introdução e sucedidos de conclusão, bibliografia, anexos e apêndices.

Assim, no primeiro capítulo constituiremos uma base teórica com o intuito de clarificar os conceitos essenciais da investigação, sendo este um elemento fundamental para a compreensão de todo o conteúdo subsequente. No segundo capítulo abordaremos os vários exemplos em que a IA é usada com uma finalidade securitária, quer no âmbito europeu como não europeu. Serão igualmente debatidas quais as vantagens e desafios inerentes ao seu uso. No terceiro capítulo apresentaremos a estratégia metodológica utilizada para alcançar os objetivos pré-estabelecidos. Procuraremos averiguar a perceção de vários especialistas referente à utilização de IA no combate ao terrorismo, culminado no quarto capítulo com a apresentação e discussão dos resultados.

Assim sendo, a questão central da nossa investigação é: qual é o papel da IA no combate ao terrorismo em Portugal? Serão ainda respondidas às seguintes questões: serão necessárias ferramentas de IA em Portugal? Quais as vantagens e desafios na utilização de IA no combate ao terrorismo?

[1] Estudo científico dos algoritmos e modelos estatísticos que os sistemas informáticos utilizam para realizar uma tarefa específica que não foi explicitamente programada inicialmente, existindo um desempenho de aprendizagem automática (Mahesh, 2020).

[2] Processo de deteção e monitorização das características físicas de uma área através da medição da sua radiação refletida e emitida a uma distância (USGS, s.d).

[3] Refere-se ao ramo da informática, mais especificamente, ao ramo da inteligência artificial que tem como objetivo fornecer aos computadores capacidades de compreensão textual escrita e falada (IBM, 2020).

Capítulo I. Os conceitos de terrorismo e inteligência artificial

1.1. A ameaça terrorista

1.1.1. Conceito de Terrorismo

Uma vez que pretendemos abordar o uso de IA face à ameaça terrorista, torna-se essencial adquirir uma perceção atual e global em relação a este fenómeno. É através do seu estudo que é possível perceber a falta de consenso em uma única definição.

O uso da violência é uma das principais características do terrorismo (Chaves, 2017). No entanto, em 1988 num estudo com a finalidade de elaborar uma definição abrangente de terrorismo foram analisadas cerca de 109 definições existentes até à época (Schmid & Jongman, 1988), manifestando-se a dificuldade para uma definição consensual por várias razões: — (1) a grande complexidade e toda a perigosidade associada ao fenómeno contribuem para uma maior dificuldade do estudo do mesmo (Duque, 2016); (2) embora após um ataque os estudos realizados se multipliquem, é ainda possível observar uma escassez de investigação académica (Horgan & Braddock 2012); (3) várias têm sido as áreas com interesse no estudo do terrorismo como por exemplo a psicologia, relações internacionais, polemologia entre outras; embora tal seja benéfico, o mesmo não contribui para um consenso mas sim para uma ambiguidade baseada nas diversas áreas de estudo (Crenshaw, 1992); (4) a predominância do lado emocional que envolve um ataque é um obstáculo a uma análise objetiva do fenómeno visto que é relativamente fácil para o espectador se identificar tanto com a vítima como com o terrorista (Simões, 2004); e (5) os interesses dos Estados que patrocinam o terrorismo tentam que este seja definido de acordo com os seus próprios interesses pela comunidade internacional, ficando assim isentos de qualquer tipo de responsabilidade (Ganor, 2002).

Desta forma, as definições são diversas. Neste sentido, a apresentação de algumas definições de autores e académicos conceituados nos estudos sobre o terrorismo, poderá contribuir para a obtenção de uma noção mais correta e precisa sobre a realidade inerente ao fenómeno. Schimd e Jongman (1998), na sua definição englobam não só as características, como os motivos de uma organização terrorista:

> Terrorismo é um método de repetida ação violenta que visa inspirar ansiedade, empregue por grupos (semi-)clandestinos, ou atores estatais, por razões idiossincráticas, criminosas ou políticas, na qual – ao contrário do assassinato – os alvos diretos da violência não são os alvos principais. As vítimas humanas imediatas da violência são em geral escolhidas aleatoriamente (alvos de oportunidade) ou seletivamente (alvos representativos ou simbólicos) dentro de uma determinada população, e servem como geradores de mensagens. Processos de comunicação

> baseados na ameaça e na violência, (...) são utilizados para manipular o alvo principal (audiência(s)) tornando-o objeto do terror, de exigências, ou de chamadas de atenção, conforme prioritariamente seja pretendida a intimidação, a coerção ou a propaganda. (p. 28)

Hoffman (2006) desenvolve a definição de terrorismo atribuindo à mesma, não só um caráter nacional como também internacional:

> (…) a criação e exploração deliberada do medo através da violência ou da ameaça de violência com vista à mudança política. O terrorismo é especificamente concebido para alcançar efeitos de longo alcance psicológico para além da(s) vítima(s) ou objeto imediato(s) do ataque terrorista. Visa instalar o medo e com isso, intimidar uma "audiência alvo" que pode incluir um grupo étnico rival ou religioso, um país inteiro, um governo nacional ou partido político, ou a opinião pública em geral. (…) Através da publicidade e poder gerada pela sua violência, os terroristas procuram obter influência e poder que de outro modo não conseguem com vista à mudança política quer à escala local como internacional. (pp. 40-41)

Numa ótica transnacional, o Conselho de Segurança da Organização das Nações Unidas, através da Resolução 1566 de 2004, define o terrorismo como atos criminosos cometidos onde o objetivo é provocar a morte ou ferimentos em alvos civis (Organização das Nações Unidas, 2004). Já a Organização do Tratado do Atlântico Norte (NATO) entende por terrorismo o "uso ou ameaça do uso ilegal da força ou violência contra indivíduos ou propriedades numa tentativa de coagir ou intimidar governos e sociedades e para ganhar controlo sobre uma população e alcançar objetivos políticos, religiosos ou ideológicos" (NATO, 2016). No contexto da UE, um ataque terrorista tem como objetivo "intimidar seriamente a população, obrigar indevidamente um governo ou organização internacional a realizar ou abster-se de realizar qualquer ato, ou desestabilizar seriamente ou destruir as estruturas políticas, económicas ou sociais fundamentais de um país ou organização internacional" (Decisão-quadro 2002/475/JAI, art.º 1.º). Numa vertente mais nacional, a disposição jurídica portuguesa, através da Lei n.º 53/2003, alterada pela Lei n.º 16/2019 no art.º 2.º n.º1 define um grupo terrorista como um grupo de duas ou mais pessoas que têm como objetivo prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado. Pode ainda forçar a autoridade pública a praticar ou abster-se de um ato, ou intimidar determinadas pessoas ou população em geral. No entanto, para a tipificação de índole terrorista é ainda necessário verificar a existência de, pelo menos, um dos seguintes crimes: "crime contra a vida, integridade física ou a liberdade de pessoas" (art.º 2.º n.º 1 al. a.); "crime contra a segurança dos transportes e das comunicações"

(art.º 2.º n.º 1 al. b.); "crime de produção dolosa de perigo comum" (art.º 2.º n.º 1 al. c.); "atos que destruam ou que impossibilitem o funcionamento (...) meios ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população" (art.º 2.º n.º 1 al. d.); "investigação e desenvolvimento de armas biológicas ou químicas" (art.º 2.º n.º 1 al. e.); ou "crimes que impliquem o emprego de energia nuclear, armas de fogo, biológicas ou químicas, substâncias ou engenhos explosivos, meios incendiários de qualquer natureza, encomendas ou cartas armadilhadas" (art.º 2.º n.º 1 al. f).

Numa primeira abordagem, os Estados Unidos da América (EUA) e a EU, abordam o terrorismo da mesma forma, mas existe um ponto fulcral em que divergem. Enquanto que para a UE os atos terroristas são "atos criminosos", para os EUA os mesmos são "atos de guerra". Desta forma, o primeiro irá optar por uma abordagem criminal e o segundo, uma militar (Jackson, 2007).

Moreira (2004) usa um provérbio chinês antigo para explicar o exercício da violência sobre inocentes como estratégia psicológica – "mata um para amedrontares dez mil" (p. 121). Apesar de todas as diferenças, o recurso à violência e o "martírio dos inocentes" (Moreira, 2004, p. 121), serão os dois elementos que permanecerão nas várias estratégias de terror, acabando mesmo por agravar-se (Liberal, 2012).

Enquanto os pontos de vista sobre o ato terrorista forem vários, várias serão as formas de combate, podendo algumas ser eficazes e outras não. Procedimentos jurídicos como a extradição, julgamento e penalização dos envolvidos torna-se extremamente difícil (Liberal, 2012). Ganor (2002) acrescenta ainda que, com uma definição partilhada entre os vários Estados, as convenções internacionais seriam reforçadas, contribuindo para o aumento da cooperação internacional.

1.1.2. Cenário de ameaça atual

O terrorismo continua a ser uma preocupação, principalmente para os jovens que acabam por estar mais vulneráveis a episódios de violência, incluindo o terrorismo (Global Risks Report, 2021). Em 2020 o número de ataques terroristas demonstra os valores mais baixos desde 2015 como é possível verificar nas figuras 1 e 2 no anexo 1, mas comparando com 2019 o número de mortos e feridos é elevado face aos ataques registados em 2020, conforme representado na figura 3 no anexo 2. No Ocidente, os ataques terroristas têm diminuído desde 2018, voltando a descer 68%, sendo que, em 2021 foram realizados apenas 59 ataques[4], na sua maioria, de cariz político (Global Terrorism Index, 2021). Neste relatório foram ainda mencionadas questões no âmbito da radicalização e recrutamento *online* e o surgimento de novas tecnologias. Apelidados

[4] De 2007 a 2021 houve cerca de 126 740 mortes por todo o mundo, sendo que apenas 865 ocorreram no Ocidente, representando assim o valor de 0,68% - a verdade é que, devido a todos estes ataques ocorrerem fora de um contexto de conflito ou de guerra, estes números tornam-se preocupantes (Global Terrorism Index, 2022).

de *"baby wolves",* esta é a nova geração recrutada pela extrema direita[5] através das plataformas *onlines* ou redes sociais como o YouTube[6], Twitch[7], Steam[8] e DLive[9]. Os vídeos criados pelos terroristas fornecem motivação, treino e inspiração para a preparação de ataques, incluindo tutoriais de construção de engenhos explosivos. É surpreendente, em 2016, as redes sociais contribuíram através da partilha de propaganda extremista para 90% dos casos de radicalização. Por fim, Liang (2022) afirma que atualmente os países estão a passar por grandes dilemas referentes às medidas de contra terrorismo e ao seu equilíbrio com o respeito pelos valores democráticos, enfatizando a necessidade de atenção para as várias tecnologias emergentes e que, "(…) embora a internet e as redes sociais pareçam muito mais inócuas do que a dinamite, estas podem ser consideradas a dinamite social desta geração" (p. 76).

A nível europeu, o TE-SAT referente ao ano de 2021, retrata que o número de ataques terroristas, na sua maioria, manteve-se estável; o número de detidos desceu significativamente estando este valor bastante associado à COVID-19; que os *jihadistas*[10] que operam *online* continuam a lutar para reconstruir a sua rede *online* depois de em 2019 o Telegram[11] ter eliminado grupos extremistas; que os suspeitos detidos por planearem ataques de extrema direita são cada vez mais novos, alguns até menores, estando associados a comunidades *online* transnacionais de violência como plataformas de jogos *online*; por fim, o COVID-19 não alterou o *modus operandi* do terrorismo, apenas contribuiu para o aumento de consumo *online* de conteúdo extremista. Ainda neste âmbito, grupos como os da extrema direita e de esquerda, utilizam estes meios para financiar as suas atividades, tendo passado vagamente para a utilização de moeda criptográfica[12], mais especificamente a Bitcoin[13] visto, muitas das vezes, o acesso a sistemas bancários serem limitados. (TE-SAT, 2021).

Por fim, no âmbito nacional, devido não estar ainda disponível o Relatório Anual de Segurança Interna (RASI) referente ao ano de 2021, foi utilizado o de 2020, sendo possível verificar que o grau de ameaça terrorista manteve-se moderado no ano de 2019, não se prevendo

[5] Ideologia política que se foca nos seguintes elementos: nacionalismo, fascismo, racismo, antissemitismo, anti imigração, nativismo e xenofobia. Grupos por norma bastante autoritário e historicamente anti comunistas. Forte tendência para mudar a ordem já estabelecida e favorecer pilares tradicionais (Weiman & Masri, 2020).
[6] Plataforma de partilha de vídeos *online* (Youtube, s.d).
[7] Serviço de transmissão de vídeo ao vivo que se centra, na sua maioria, na transmissão ao vivo de jogos, no entanto as transmissões podem ser de todo o tipo (Twitch, s.d).
[8] Serviço de distribuição digital de jogos, funcionado também como rede social (Steam, s.d).
[9] Serviço de transmissão ao vivo de vídeo (DLive, s.d).
[10] Jihadismo é definido como uma subcorrente violenta do Salafismo que rejeita a democracia e parlamentos eleitos. A legislação humana está em variação com o estatuto de Deus, o único legislador. O seu objetivo é criar um Estado Islâmico governado exclusivamente por islâmicos. Os principais representantes dos grupos jihadistas são a Al-Qaeda e o grupo terrorista autoproclamado Estado Islâmico (TE-SAT, 2021).
[11] Serviço de mensagens instantâneas (Telegram, s.d).
[12] Meio de troca, centralizado ou descentralizado, onde através da criptografia ou tecnologia de blockchain, as validades de transações são asseguradas e novas unidades de moedas criadas (Boof & Ferreira, 2016).
[13] Tipo de moeda criptográfica (Boof & Ferreira, 2016).

qualquer alteração do mesmo (Sistema de Segurança Interna, 2020), tal não significa a inexistência de investigação referente a formas de combate ao terrorismo. Aliás, não é descartada a possibilidade de a ameaça terrorista visar alvos ou interesses de estrangeiros que estejam a viver em território nacional (Sistema de Segurança Interna, 2020). O RASI de 2020 também menciona o contributo da pandemia para o aumento da exposição à radicalização e ao ativismo *online*.

Como medidas para as problemáticas apresentadas, a Europol desenvolveu um conjunto de ferramentas e, em 2016 é criado o *European Counter Terrorism Centre* (ECTC) com uma abordagem baseada em quatro pilares, a saber — i) facilitação na troca de informações e cooperação entre fronteiras; ii) apoio operacional, coordenação e *expertise* eficaz; iii) mitigação proativa do uso de redes sociais para fins de radicalização e suporte da análise operacional em investigações *online*; e iv) capacidade central de apoio estratégico. De modo a atingir os seus objetivos, são utilizadas tecnologias de reconhecimento facial para detetar criminalidade organizada e terrorismo, para identificar suspeitos desconhecidos e desenvolver novas pistas de inteligência. Existe igualmente um programa de rastreamento de recursos financeiros de terroristas, usado desde 2010, não só entre a UE, mas também entre os EUA, permitindo o mapeamento das várias redes terroristas. São também desenvolvidas investigações e análises com base em comunicações da internet. Existe ainda a *EU Internet Referral Unit* (EU IRU) que pertence ao ECTC e coordena esforços para limitar o acesso a propaganda terrorista *online* através da partilha de boas práticas e uniformização de processos. Está constantemente a rastrear inovações desenvolvidas pelos grupos terroristas, a monitorizar as redes sociais e canais com o auxílio de especialistas em linguagem onde o foco é a linguagem não europeia (TE-SAT, 2021). O ECTC coopera com países associados do espaço Schengen, EUA, organizações internacionais como a INTERPOL, Balcãs Ocidentais, Médio Oriente, Norte de África e responsáveis pela produção de investigação académica.

1.2. Inteligência Artificial

1.2.1. Conceito de Inteligência Artificial

A expressão “Inteligência Artificial” foi criada por John McCarthy em 1956, porém, o seu desenvolvimento surge após a Segunda Guerra Mundial (Russel & Norving, 2010). Este conceito, semelhante ao de terrorismo também não é consensual, existem algumas características que estão, quase sempre presentes, nomeadamente a autonomia, a capacidade de resolução de problemas e de um planeamento mais complexo, possibilidade de raciocínio, tomada de decisão, previsão, monitorização, aprendizagem por experiência, adaptação a novas situações, compreensão de linguagem, argumentação, reconhecimento visual e/ou auditivo e reconhecimento de objetos (Fundação para a Ciência e Tecnologia, 2021). A IA não se limita a entender situações, esta constrói entidades inteligentes que raciocinam, fazem escolhas e tomam

decisões, pertencendo à família de tecnologias de rápida evolução (Regulamento do Parlamento Europeu e do Conselho, 2021). Em 2018, na sua comunicação sobre a IA para a Europa, a Comissão Europeia (2020a) apresentou a seguinte definição:

> O conceito de IA aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos. Os sistemas baseados em IA podem ser puramente confinados ao *software*, atuando no mundo virtual (por exemplo, assistentes de voz, programas de análise de imagens, motores de busca, sistemas de reconhecimento facial e de discurso), ou podem ser integrados em dispositivos físicos (por exemplo, robôs avançados, automóveis autónomos, veículos aéreos não tripulados ou aplicações da Internet das coisas (p. 1)

Esta definição foi depois aperfeiçoada pelo Grupo de Peritos de Alto Nível (Comissão Europeia, 2020a):

> Os sistemas de inteligência artificial (IA) são sistemas de *software* (e eventualmente também de *hardware*) concebidos por seres humanos, que, tendo recebido um objetivo complexo, atuam na dimensão física ou digital percecionando o seu ambiente mediante a aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido. Os sistemas de IA podem utilizar regras simbólicas ou aprender um modelo numérico, bem como adaptar o seu comportamento mediante uma análise do modo como o ambiente foi afetado pelas suas ações anteriores (p. 8)

Nos sistemas de IA existem dois componentes importantes – sensores e algoritmos. Nos sensores existem teclados, câmaras, microfones, sensores de movimento, de temperatura ou de pressão, ou seja, tudo aquilo que permite ao sistema interagir com o ambiente, gerando dados de uma forma mais rápida (Fernandes, 2020). Os algoritmos são sequências de instruções e o seu desempenho depende do conjunto de dados utilizados na sua fase de treino e de teste, permitindo que os algoritmos de aprendizagem automática identifiquem correlações entre os dados e posteriormente sejam criadas previsões.

Ao conjunto de dados utilizados chama-se *big data* – algo fluído e em permanente expansão e desenvolvimento (Neiva, 2020). Há três características inegáveis: grande volume de dados que este agrega, variedade e velocidade com que estes são processados, o seu formato e estrutura (Chan & Moses, 2015). Gonçalves (2017) explica que os dados são analisados em

tempo real, são exaustivos, abrangentes e detalhados. Depois, são convertidos em algoritmos categorizados numericamente para, posteriormente, extrair informação que permitam orientar políticas criminais (Araújo, 2008).

Ainda no âmbito do conceito de IA, a própria definição varia de acordo com a época e com os objetivos estabelecidos de quem trabalha com esta. Existe uma tentativa de recriar o pensamento humano ou o comportamento humano? A finalidade é desenvolver uma máquina semelhante ao ser humano com todas as suas capacidades? Russel e Norving (2010) preferem uma abordagem mais racional e focada para o comportamento, sendo o ideal um agente inteligente capaz de escolher a melhor resposta possível para cada situação. Não existe uma definição única, a história da IA é constituída por diferentes ciclos com várias abordagens criativas juntamente com uma constante melhoria das teorias mais recentes (Russel & Norving, 2010). Estas duas vertentes, humana e racional, dividem-se em agir e pensar humanamente e agir e pensar racionalmente.

Agir humanamente é uma abordagem realizada através das ciências empíricas que envolve hipóteses e confirmações retiradas de experiências. Um exemplo é o Teste de Turing, desenvolvido por Alan Turing em 1950. Este explica que o comportamento inteligente é a habilidade de atingir um grau de ação semelhante à performance humana em todas as tarefas cognitivas sendo dessa forma possível enganar um pessoa, ou seja, um jogador humano entra numa conversa em linguagem natural, com outro humano e uma máquina estando todos os participantes separados um dos outros. Caso o jogador principal não consiga distinguir a máquina do humano, a máquina passa no teste. O modo de conversação é restrita a um instrumento de texto, seja um teclado ou uma tela. O teste completo exige contacto visual, porém há uma grande dificuldade em realizar o mesmo com sucesso visto que, para este contacto ser bem sucedido, ou seja, o interrogador ser enganado, é necessário que a máquina entenda as convenções normais da interação humana, coisa até agora, impossível.

Por outro lado a vertente pensar humanamente é realizada através de uma abordagem mais cognitiva, ou seja, quando se afirma que o programa pensa como um ser humano é necessário criar formas de determinar como é que este pensa – ou através de técnicas de introspeção numa tentativa de “agarrar” os pensamentos para seja possível analisar os mesmos ou através de experiências psicológicas. Todas estas opções são difíceis de realizar, só quando uma teoria suficientemente precisa relativamente a estes processos existir é que tal pode ser transmitido para as máquinas (Russel & Norving, 2010). O futuro é promissor e a ciência cognitiva e a IA têm desenvolvido esforços em conjunto, principalmente para melhorar as áreas da visão, linguagem natural e aprendizagem.

Nas vertentes mais racionalistas, no pensamento racional existe uma combinação entre a matemática e a engenharia. Aristóteles foi o primeiro filósofo grego a tentar codificar aquilo que se apelidava de “pensar corretamente”. Através dos seus silogismos foi possível criar padrões

para determinadas estruturas de argumentos que acabavam por dar sempre as mesmas conclusões face a premissas corretas – o objetivo era governar operações da mente e trabalhar o campo da lógica. Por volta de 1965 acreditava-se que determinados programas, existindo memória e treino, com a descrição de um problema através de uma notação logística era possível encontrar uma solução para o mesmo. E se não houver qualquer tipo de solução? A máquina poderá nunca parar de a procurar (Russel & Norving, 2010). Surgem ainda outros dois obstáculos – (1) não é fácil utilizar informação informal, mais subjetiva e transformar a mesma numa notação de lógica, principalmente quando é uma questão onde não existem certezas de determinado conhecimento; (2) existe uma grande diferença entre ser capaz de resolver um problema e ser capaz de o resolver na prática. Esta última dúvida surge através de outra questão - o que significa agir racionalmente? É quando se age através de uma crença, ou seja, existe uma perceção de determinada informação e depois existe uma ação. Fazer inferências corretas faz parte do agente que é racional visto que agir racionalmente é racionalizar logicamente que determinada ação vai permitir a realização de determinado objetivo. Tal nem sempre é fácil, por vezes estas inferências corretas não são baseadas apenas em racionalidade visto que, em determinadas situações, não existe algo correto para se fazer mas algo que deve ser feito, uma decisão que deve ser tomada. Outra dificuldade dos investigadores é o facto de que, em determinadas situações agir com racionalidade não é o mais benéfico nem o mais fácil — situações de reflexos (uma mão que se queima numa superfície quente, neste caso, uma resposta mais deliberada onde existe uma tentativa de realizar um pensamento racional não é o mais indicado, acabando por trazer apenas prejuízos). Estas são apenas algumas abordagens que nos permitem ter pontos de vistas completamente diferentes sobre um conceito tal como também sobre as suas próprias limitações.

Existe a ideia de que a IA foi desenvolvida mais recentemente e é associada a imagens de robôs ou computadores super inteligentes, a verdade é que a origem desta está presente em áreas que à partida não parecem ter qualquer ligação com o próprio conceito. De acordo com Oliveira (2019) foi há cerca de 2000 anos, através das teorias da racionalidade e da aprendizagem na área da filosofia que são dados os primeiros passos com a crença de que a mente pode ser igual à máquina operando através de conhecimento, num determinado código com determinado significado, o que permite tomar decisões corretas. De seguida, há 400 anos, através das teorias formais da lógica, probabilidades, tomada de decisões e computação, e ainda dos ramos da matemática, são feitos alguns desenvolvimentos que tornam possível manipular situações de lógica em situações de incerteza e probabilidade. Mais tarde, com o surgimento da psicologia foi possível aprender como a mente humana funciona, como é que esta pensa, raciocina, toma decisões, transformando essa aprendizagem em novas teorias. A linguística é responsável por teorias referentes à própria estrutura da linguagem e dos seus significados e por fim, surgem as ciências computacionais que permitiram tornar real a IA, ou seja, desenvolver ferramentas que permitissem colocar em práticas todas as teorias anteriormente criadas.

1.3. Abordagem da Europa com a Inteligência Artificial

Na Dinamarca, os serviços de emergência conseguem diagnosticar paragens cardíacas ou outros problemas com base na voz de uma chamada; na Áustria, radiologistas detetam tumores com maior exatidão; explorações agrícolas controlam a circulação, a temperatura e o consumo de alimentos dos animais. Em suma, os fabricantes europeus tornam-se mais eficientes e eficazes (Comissão Europeia, 2018). Estes são pequenos exemplos da utilização de IA. No âmbito do terrorismo, a IA pode identificar propaganda terrorista *online*, descobrir transações suspeitas na venda de produtos perigosos, identificar objetos perigosos ocultos ou substâncias ou produtos ilícitos, prestar assistência a cidadãos em emergência e ajudar equipas de primeira intervenção (Comissão Europeia, 2020a). Também pode ser benéfica para formação e treino, quer militar, quer civil, tal como para o aumento da autoproteção do pessoal militar, permitindo que estes se mantenham à distância durante os ataques (Parlamento Europeu, 2020).

Após o reconhecimento das potencialidades da IA, o objetivo da EU é ser líder nesta matéria. Já existe algum quadro regulamentar sólido e fiável em matéria de segurança e de responsabilidade dos produtos a circular na União Europeia, mas a IA, a *internet of things*[14] e a robótica estão a transformar as características de muitos produtos e serviços (Comissão Europeia, 2020a), é necessário criar um quadro jurídico claro e previsível para dar respostas aos vários desafios, tal como a criação de debates internacionais (Parlamento Europeu, 2020).

A comunicação realizada em 2018 pela Comissão Europeia referente à IA define uma iniciativa europeia que visa reforçar a capacidade industrial e tecnológica da UE, a adoção da IA na economia, visa estudar as mudanças socioeconómicas e, por fim, visa garantir a criação de um quadro jurídico e ético adequado (Comissão Europeia, 2018).

Comparando o investimento dos EUA de 6 500 milhões a 9 700 milhões de euros na Ásia e de 12 100 milhões a 18 600 milhões de euros na América do Norte, a UE está atrasada com investimentos de 2 400 milhões e 3 200 milhões de euros (McKinsey Global Institute, 2017). De facto, a EU alberga profissionais especialistas que fazem parte de grandes comunidades de investigação, com especial destaque para a robótica, porém, acabam por trabalhar fora do espaço europeu fazendo com que a EU seja consumidora de soluções desenvolvidas nesses mesmos países. Assim, a Comissão Europeia (2018) enumerou alguns objetivos: atrair investimento público ou privado; reforçar a investigação e a inovação dos laboratórios; apoiar centros de investigação; levar a IA a pequenas empresas e potenciais utilizadores; apoiar a realização de testes e disponibilização de mais dados.

A IA pode facilitar a vida aos trabalhadores, auxiliando-os a executar tarefas repetitivas, cansativas e até mesmo perigosas, permitindo que, num tecido social envelhecido, as pessoas

[14]Uma rede aberta e abrangente de objetos inteligentes que têm a capacidade de se auto-organizar, partilhar informações, dados e recursos, reagir e agir face a situações e mudanças no ambiente (Madakam et al., 2005, p. 165).

possam permanecer no mercado durante mais tempo, incluindo até pessoas com deficiência. Como tal, é necessário ajudar os cidadãos a desenvolveram competências digitais e outras que apenas podem ser desempenhadas por humanos como a supervisão[15], pensamento crítico e criatividade. Deve igualmente apoiar aqueles que poderão ver os seus postos de trabalho a serem substituídos (Miguéns, 2016).

De modo a atingir os seus objetivos a Comissão desenvolveu a Aliança Europeia para a IA, um grupo com interessados e peritos, com vista à elaboração de um projeto de orientações para as questões relacionadas com a ética e os direitos fundamentais, em colaboração com o Grupo Europeu de Ética para as Ciências e as Novas Tecnologias. Foi criado um documento de orientação referente à interpretação da Diretiva Produtos Defeituosos[16] à luz da evolução tecnológica. Foi ainda criado um relatório sobre as implicações mais abrangentes para os quadros regulamentares em matéria de segurança e de responsabilidade decorrentes da IA, eventuais lacunas e orientações. Sob recomendação do Parlamento Europeu, foi apoiada a investigação da explicabilidade[17] na IA tal como criado um projeto para a sensibilização dos algoritmos, preconceitos e discriminação nos processos de tomadas de decisões autónomas. Por fim, com o apoio do Grupo Consultivo Europeu dos Consumidores e do Comité Europeu para a Proteção de Dados, foi pedido um auxílio para os consumidores e autoridades de supervisão em matéria de proteção de dados. A Aliança Europeia para a IA irá interagir com o Parlamento Europeu, Comité Económico e Social Europeu e o Comité das Regiões e outras organizações internacionais — O plano de cooperação internacional propõe cerca de 70 ações conjuntas para uma cooperação mais estreita e eficaz (Comissão Europeia, 2020a). Aliás, em outras instâncias multilaterais — Conselho da Europa, a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), a Organização para a Cooperação e Desenvolvimento Económico (OCDE), a Organização Mundial do Comércio (OMC) e a União Internacional das Telecomunicações (UIT) — estão a decorrer atualmente vários trabalhos referentes ao uso da IA (Comissão Europeia, 2020a).

1.3.1. Medidas a desenvolver de acordo com a Comissão Europeia

Todos os Estados-Membros salientam que não existir um quadro europeu comum referente à IA (Comissão Europeia, 2020a), comporta dificuldades várias. A própria definição de IA e de

[15] Supervisão humana é essencial para evitar situações como as de Robert McDaniel. A Polícia de Chicago entra em contacto com McDaniel para informar que o algoritmo teria produzido uma lista de 400 potenciais suspeitos de estarem envolvidos em crimes violentos. McDaniel teria sido categorizado com valores de 215 a 500. Consequentemente, foi vigiado e avisado para evitar qualquer prática de infração ou crime. Após uma análise foi possível concluir que este alerta surgiu erradamente devido a uma associação deste com os seus vizinhos que estavam anteriormente associados à prática de crimes violentos. McDaniel apenas teria tido problemas relacionados com o uso de estupefacientes e não violência (Liv, n.d)

[16] Decreto-Lei n.º 383/89, Diário da República n.º 255/1989, Série I de 6 de novembro de 1989 – Responsabilidade decorrente de produtos defeituosos.

[17] Ou *explainability.*

ferramenta de alto risco gera dúvidas. De acordo com a Comissão Europeia (2020a), um sistema de IA deve ser considerado de alto risco se cumprir dois critérios — (1) o sistema é utilizado num setor em que, dadas as características das atividades tipicamente realizadas, é expectável que ocorram riscos, devendo esta lista ser constantemente revista e alterada se necessário; (2) a forma como o sistema é utilizado é favorável à ocorrência de riscos significativos. Esta avaliação também pode basear-se no impacto que a ferramenta pode ter para os direitos dos envolvidos, independentemente do setor em que está a ser aplicada. Um exemplo poderá ser o recurso a identificação biométrica à distância[18] e de outras tecnologias de vigilância intrusivas (Comissão Europeia, 2020a).

Foram assim criados requisitos que devem ser aplicados na implementação ou criação de um sistema de IA, sejam estes desenvolvidos ou não na EU. No que diz respeito aos dados utilizados para treino, os valores da Europa devem ser respeitados, nomeadamente os direitos e liberdades dos cidadãos consagrados na Carta dos Direitos Fundamentais da UE, na Convenção Europeia dos Direitos Humanos e a jurisprudência do Tribunal Europeu dos Direitos Humanos (Parlamento Europeu, 2019). Na conceção de IA, existem dois *slogans*: «ética desde a conceção» e «segurança desde a conceção». Estes representam os princípios éticos e legais que são implementados e garantidos (Comissão Europeia, 2018). Estes dados devem ser suficientemente amplos e abranger todo o tipo de cenários possíveis. Muitas vezes, os registos digitais existentes do comportamento humano permitem inferir a idade, género, orientação sexual, religião ou opinião política dos indivíduos, como tal é necessário assegurar à população que os seus dados são controlados e nunca utilizados para as prejudicar ou discriminar (Comissão Europeia, 2019). Nesta ótica, é necessário que a transparência seja assegurada, sendo possível obter uma explicação do processo de tomada de decisão (Comissão Europeia, 2019). Consequentemente, a Comissão convida o Comité Europeu para a Proteção de Dados a elaborar orientações relativas ao tratamento de dados pessoais nesta temática (Comissão Europeia, 2018b).

De seguida, todos os registos e dados devem ser conservados de modo a que, ações potencialmente problemáticas possam ser identificadas e verificadas. Estes registos serão conservados durante um período limitado razoável para assegurar a proteção de informações confidenciais. Todos os utilizadores destas ferramentas devem ter conhecimento sobre as capacidades e limitações das mesmas. É de salientar que todos estes sistemas devem ser robustos, exatos e seguros, ou seja, garantir que podem lidar adequadamente com erros, incoerências e ataques durante todas as fases de vida. Devem garantir também a segurança, física e mental, de todas as partes envolvidas e, em caso de acidente, a reversibilidade de

[18] Dados biométricos são definidos como «dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitem obter ou confirmar a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos (Diretiva sobre a Proteção de Dados na Aplicação da Lei, artigo 3.º, n.º 13; RGPD, artigo 4.º, n.º 14; Regulamento (UE) 2018/1725, artigo 3.º, n.º 18) (Parlamento Europeu e Conselho da União Europeia, 2016a).

consequências (Comissão Europeia, 2019). Nesta linha de pensamento surge a importância da criação de mecanismos de responsabilização em caso de acidente através da constante fiscalização e disponibilidade de dados para as falhas serem identificadas (Comissão Europeia, 2019a). De acordo com a Comissão Europeia (2020a), é necessário que exista um conjunto de obrigações dirigida a(aos) interveniente(s) que estão em melhor posição para fazer face aos potenciais riscos. Por fim, é relevante existir sempre uma visão humana, estes sistemas devem "agir como facilitadores de uma sociedade próspera e equitativa, apoiando a atividade humana e promovendo os direitos fundamentais, e não reduzindo, limitando ou guiando a autonomia humana" (Comissão Europeia, 2019, p. 4). Todas as decisões realizadas por IA só ganham valor se previamente analisadas e validadas por um humano (Comissão Europeia, 2020).

Interessa especificar quais os requisitos específicos para a utilização de identificação biométrica à distância. Em matéria de proteção de dados, as regras de UE proíbem o tratamento de dados biométricos para efeitos de identificação inequívoca de uma pessoa singular, exceto em condições específicas, nomeadamente por razões de interesse público. Neste caso, o tratamento deve ser efetuado com base no direito europeu ou nacional, cumprindo sempre os requisitos em matéria de proporcionalidade, direito à proteção de dados e prestação de garantias adequadas (Comissão Europeia, 2020a).

Por fim, é pertinente que as administrações públicas (hospitais, supervisores financeiros, transportes, e outros domínios de interesse público) comecem rapidamente a utilizar produtos e serviços baseados em IA (Comissão Europeia, 2020a).

Todas estes requisitos, ações e planos devem ser sempre desenvolvidos de acordo com os princípios da responsabilidade, equidade, governabilidade, precaução, responsabilização, imputabilidade, previsibilidade, rastreabilidade, fiabilidade, transparência, explicabilidade, capacidade para detetar eventuais alterações nas circunstâncias e no ambiente operacional, distinção entre combatentes e não combatentes e proporcionalidade (Parlamento Europeu, 2020).

Capítulo II. A ameaça do terrorismo e o combate por meios tecnológicos

2.1. *Lone Wolves*, radicalização e a Internet

Para além dos terroristas que se enquadram numa rede hierarquizada, onde a forma de obtenção de meios exige várias fases e vários elementos, existem os *lone wolves* ou lobos solitários. O seu modo de atuação é diferente porque atuam sozinhos, tanto no ataque como no planeamento, tornando-se numa grande ameaça. Autores como Bakunin (1980) afirmavam que um revolucionário deveria agir sozinho ou em grupos pequenos por iniciativa própria, de modo a não chamar à atenção das autoridades. O lobo solitário, segundo Bakker e Zuikdewijn (2015) representa a ameaça ou uso de violência por um único autor, não agindo por razões meramente pessoais, onde o seu objetivo é influenciar um público mais amplo. Este age sem qualquer tipo de apoio no planeamento, preparação e execução do ataque, tal como a sua decisão não é uma ordem vinda de uma cadeia superior hierárquica, podendo ser inspirada por outros. Desta forma, é através de um exemplo de uma pequena mudança no modo de atuação que surge um tipo de ameaça completamente diferente, como tal, a resposta deve ser também ajustada. Face ao exposto, a inteligência mudou o seu foco de procura, ao invés de procurar um padrão nos alvos e na forma de atuação, procura outro tipo de marcadores como a mudança de comportamentos ou aparência, o aumento ou diminuição de uma determinada atividade, o estabelecimento de novas ligações e contactos, entre outras (Ganor, 2021).

Sendo o terrorismo um fenómeno dinâmico e em constante adaptação, para além da existência de novos atores como os lobos solitários, o próprio processo de radicalização altera-se. Este torna-se mais simples, fácil e rápido, sem qualquer tipo de contacto físico e até mesmo, sem qualquer interveniente, ou seja, auto radicalização (Behr, 2013) – passa-se a estar num espaço onde as pessoas tudo podem dizer ou fazer sem qualquer tipo de consequência (Davis, 2009). Autores como Sageman, (2008) afirmam que a radicalização presencial foi substituída pela radicalização *online*.

Num breve estudo realizado por Jensen (2018), ao analisar as redes sociais de 478 extremistas rapidamente se percebe um aumento gradual do uso da internet — de 2005 a 2010, apenas um quarto usou redes sociais e apenas foi a causa primária de radicalização em 1% dos casos. De 2011 a 2016, o uso subiu para 76% e foi a causa principal de 17% dos casos. Já de 2015 a 2016, 85% usavam internet, tendo esta um grande papel na maioria dos casos de radicalização. A título de exemplo, em Madrid, um homem de 34 anos abandonou o seu trabalho para se dedicar ao consumo de propaganda terrorista, criando vários perfis falsos para espalhar conteúdo extremista, acabando depois por ser detido em 2016 (TE-SAT, 2021).

Desta forma, o Estado Islâmico terá utilizado a internet para recrutar pessoas e divulgar propaganda[19] – mais de 50 000 pessoas terão viajado pelo mundo para ir para o Estado Islâmico (Cook & Vale, 2019). A radicalização *online* tornou-se um dos maiores desafios securitários (Conselho da União Europeia, 2018). Num estudo realizado a 137 *jihadistas* franceses, ao analisar o seu percurso, foi possível confirmar que de facto a internet permite o planeamento, comunicação, acesso a propaganda, mas não existe qualquer evidência de que a radicalização exista totalmente devido e apenas à internet (Hecker, 2018) — a internet não é a grande causa, apenas um facilitador.

Aliados à radicalização surgem casos de imitação. Foi através do ataque de Andres Breivik que surge uma grande atenção mediática, principalmente através da internet, para a violência de extrema direita. Breivik era um membro de um fórum *online* neo-nazi chamado *Nordisk* onde expressava as suas ideologias publicando conteúdo de ódio e até o seu manifesto de 1516 páginas antes do ataque terrorista. Vários foram os ataques realizados tendo como fonte de inspiração os ataques em Oslo e na ilha de Utoya em 2011 (Azani et al., 2020) — Robert Bowers de 46 anos, antes do seu ataque numa sinagoga em Pittsburgh responsável pela morte de 11 pessoas e seis feridos, publicou uma última mensagem para os seus seguidores relativamente ao possível ataque; Brenton Tarrant de 29 anos, um australiano a viver na Nova Zelândia, partilhou ao vivo o seu ataque em duas mesquitas matando 51 muçulmanos e ferido 49. Tarrant terá alertado os seus seguidores sobre o ataque publicando o seu manifesto de 74 páginas – "The Great Replacement"; John Earnest, 20 anos, entrou numa sinagoga em Poway, na Califórnia vitimando uma mulher e três feridos, publicou antes do ataque um manifesto com o nome "An open letter"; Patrick Crusius de 21 anos, conduziu durante 10 horas até ao Texas para atacar emigrantes espanhóis num centro comercial, acabando também por publicar antes o seu manifesto "The Inconvenient Truth" (Azani et al., 2020).

Visto grande parte do planeamento de ataques terroristas, na sua maioria, poderem ser detetado em várias plataformas *online* (Wagner, 2005), é aqui que a Internet, e consequentemente a IA, têm um papel fundamental. A Internet é utilizada por grupos terroristas para realizar comunicações, para aceder a informações sobre os seus potenciais alvos, para obter informações mais técnicas referentes à construção de explosivos/armas, para difundir propaganda, para iniciar processos de recrutamento, para realizar ataques no ciberespaço, entre outros. Todas estas atividades permitem que as hierarquias destas redes se tornem mais fluídas e dinâmicas (Wagner, 2005). O que antes era transmitido através de cartas ou intermediários, passa hoje a ser feito de qualquer lugar do mundo, a qualquer hora do dia. Documentos encriptados com informações relevantes sobre possíveis ataques podem ser facilmente partilhados de uma forma mais segura, e melhor ainda, as contas de onde ou para onde são

[19] Consultar anexo 3, nomeadamente as figuras 4, 5 e 6 para visualização de exemplos de propaganda e atividade online exercida por grupos terroristas.

enviadas mensagens/informações podem ser constantemente eliminadas, modificadas, recriadas de modo a tornar a sua deteção mais difícil. Viagens que antes eram realizadas para adquirir o máximo de dados referentes a um alvo ou localização, podem agora ser realizadas através de vários cliques sem qualquer risco associado.

Devido à sua difícil regulamentação, a internet tem-se assumido para os terroristas como um instrumento de propaganda de grande eficácia devido aos reduzidos custos associados (Liberal, 2012). Várias são as plataformas utilizadas, a título de exemplo, o *YouTube*, *Facebook*, *Telegram* e *Dark Net*.

No *Youtube* é possível que os utilizadores vejam e publiquem vídeos, partilhem, criem listas de reprodução, comentem, reportem vídeos e subscrevam a canais de interesse. Um dos vídeos mais visto do mundo foi publicado por um grupo de extrema direita, contou com mais de 10 000 visualizações quando partilhado inicialmente, e com mais de 475 000 visualizações depois de publicado. Foi possível verificar que em 360 canais analisados 331 849 vídeos continham conteúdo extremista contribuindo assim para a radicalização dos seus utilizadores (Weiman & Masri, 2020).

Uma das plataformas mais importantes no âmbito da organização e comunicação política através de debates e troca de opiniões, é o *Facebook*. Esta está constantemente a tentar eliminar conteúdo de ódio e extremista, mas vários são os desafios. Em março de 2019, numa sexta feira, às 13:30, um ataque em massa na Nova Zelândia realizado por Brenton Tarrant foi partilhado em direto obtendo comentários como “boa sorte”, “parece divertido” e “melhor forma de começar a semana”. Cerca de 200 pessoas terão assistido ao vídeo em direto de 17 minutos. Este foi ainda visualizado pelo menos 4 mil vezes antes de o Facebook o retirar e nas 24 horas seguintes foram removidos cerca de 1,5 milhões de cópias do mesmo. Numa simples pesquisa foi possível verificar a existência de mais de 500 grupos e páginas relacionados com a extrema direita, provenientes de França, Alemanha, Itália, Reino Unido, Polónia e Espanha (Weiman & Masri, 2020).

Considerado um paraíso para os terroristas, totalmente encriptado e não monitorizado, surge a plataforma *Telegram* em 2013. Em 2019 esta eliminou grupos extremistas porém, um grupo apelidado de *Terrorgram*, conseguiu juntar 4 mil seguidores num ano. Aqui seriam partilhados desenhos, imagens, vídeos e bibliotecas *onlines* (Weiman & Masri, 2020). É de salientar que, nesta plataforma, existe uma nova forma de disseminação de conteúdo – uma espécie de sistema de IA que gera propaganda através de aprendizagem de documentos extremistas que são escritos. Esta ferramenta aprende a imitar os seus escritores criando constantemente novo conteúdo (Azani et al., 2020).

Para além destas plataformas mencionadas anteriormente, existe uma zona considerada ainda mais segura — a *Dark Net*. Visualizando a internet como um grande *iceberg*, na ponta existe aquilo que é possível observar, porém, submerso está toda uma parte não acessível —

Deep Web – abaixo desta está situada a *Dark Net* que alberga conteúdo ilegal não sendo o seu acesso fácil (Weimann, 2018). Neste espaço existem redes sociais semelhantes às mencionadas anteriormente, no entanto, sem qualquer tipo de controlo (Weiman & Masri, 2020). Na *Dark Net* existe todo o tipo de propaganda, desde publicações a explicar como desenvolver armas biológicas e explosivos.

Para além da propaganda, o próprio trabalho de pesquisa e planeamento passa a ser realizado *online*. O manual de treino da Al-Qaeda explica que 80% das informações sobre o inimigo podem ser adquiridas em fontes públicas e abertas (Conway, 2006). A quantidade de mapas, imagens, edifícios governamentais, monumentos históricos, rotas de transportes, sistemas de abastecimento de água, juntamente com a informação geoespacial e as tecnologias de satélite permitem uma alteração na forma de vigilância e reconhecimento (Tibbetts, 2002). Thomas (2003) explica que os computadores apreendidos à Al-Qaeda no Afeganistão retratavam que todo o ataque de 11 de setembro de 2011 foi realizado com informação disponível na internet, tendo sido trocados milhares de e-mails criptografados (Weimann, 2005). Numa primeira fase, determinados dados podem parecer insignificantes, porém, após decifrar dados encontrados nos computadores dos responsáveis pelo atentado ao World Trade Center em 1993 ajudaram a descobrir planos que estariam em curso para a operação Milénio[20], em 2000 na Jordânia (Jessee, 2006).

2.2. Ferramentas de inteligência artificial no combate ao terrorismo

É possível concluir através dos capítulos anteriores que é na internet que as FSS têm uma grande oportunidade para detetar novos indivíduos suspeitos pela prática de terrorismo.

Existe um conjunto de comportamentos de alerta em algumas das publicações *online* realizadas por terroristas, como por exemplo, a fixação, a identificação e o vazamento (Meloy et al., 2012).

Na fixação existe uma preocupação crescente com determinada pessoa ou causa. Esta é avaliada através da utilização de algumas palavras-chaves, relacionando-as com outras organizações ou entidades (Mullen et al., 2009).

Na identificação existe a crença e a mentalidade de guerreiro, onde o *lone wolf* será o único agente responsável e pronto para a mudança (Meloy et al., 2001). É nestes dois campos que são desenvolvidas ferramentas semiautomáticas de pesquisa e técnicas de mapeamento de modo a identificar quais os fóruns e utilizadores que devem ser monitorizados com mais atenção (Cohen et al., 2014). Surge assim como exemplo a plataforma desenvolvida pela *Totalförsvarets forskningsinstitut* (*Swedish Defence Research Agency*), que concluiu que existem alguns marcadores comportamentais a seguir: ações preparatórias, expressões linguísticas de atitude,

[20] No início de 2000, vários ataques terroristas associados ao Al-Qaeda foram planeados no contexto das celebrações do milénio em quatro locais turísticos na Jordânia (ABC News, 2007).

motivações e intenções (Cohen et al., 2014). Relativamente à linguagem, a título de exemplo, é possível observar uma constante utilização do pronome "nós" para autoidentificação e de "eles" para identificação do grupo adversário. Foi igualmente observado a utilização de palavras como "honra", "dever" e "justiça" (Pennebaker & Chung, 2008). O benefício na análise linguística é o facto de que as pessoas não conseguem facilmente alterar os padrões de uso da língua (Chung & Pennebaker, 2011). Outro exemplo é a ferramenta de rápida tradução de conteúdo extremista (Cohen et al., 2014). O mesmo autor destaca ainda outras duas ferramentas (1) análise de sentimentos através de algoritmos computacionais que permitem distinguir documentos/comentários radicais ou não radicais; (2) mapeamento de várias páginas da internet. É através do *crawling*[21] que várias correspondências podem ser detetadas, priorizando assim pessoas de interesse. Não menos importante surge a ferramenta de reconhecimento de autor. De modo a dificultar a sua procura, estes atores criam vários perfis em vários fóruns. Porém, através de algoritmos é possível analisar a frequência de determinadas palavras e construções sintáticas de modo a criar uma espécie de perfil relativamente ao estilo de escrita, permitindo depois associar esta a determinado sujeito (Brynielsson et al., 2013). O estilo de escrita permite também descobrir atributos de pessoas como a idade (Pennebaker & Stone, 2003), género (Newman et al., 2008), estado de saúde (Pennebaker & Mayne, 1997) ou o estado emocional (Alpers et al., 2005).

Por fim, o terceiro comportamento observável é o vazamento de informação, considerado um dos pontos mais cruciais na prevenção destes ataques. Muitas vezes, os lobos solitários distribuem as suas ideias e manifestos revelando as suas visões extremistas e intenções, seja através de canções, diários, poemas ou tatuagens (Spaaij, 2015) – cerca de 46% dos *lone wolves* partilham essas informações (Ellis et al., 2016). De facto, em cerca de 83% dos ataques realizados por lobos solitários, terceiros tinham conhecimento das suas opiniões extremistas (Gill et al., 2014). Um bom exemplo é o caso recente (30 de novembro em 2021) de um atacante ativo na escola secundária de Oxford em Michigan — (1) o atirador terá postado várias mensagens e uma foto de uma arma que foi usada para realizar o ataque; (2) este publicou a seguinte mensagem na rede social Instagram[22] "agora torno-me na morte — destruidor do mundo — vemos nos amanhã Oxford"; (3) dois dias antes do ataque, dois professores reportaram a sua mudança repentina de comportamento, afirmando que este estaria a partilhar ideias extremistas com os seus colegas; (4) horas antes do ataque, outro professor realizou uma reunião com o atirador e os seus pais visto que os seus comportamentos estariam a piorar, mas o aluno voltou para as aulas; (5) depois do ataque foram descobertos dois vídeos feitos pelo atirador onde este explicava em detalhe como iria realizar o ataque e matar os colegas; (6) na sua mochila foi encontrado um diário onde estava exposto o seu desejo de matar vários alunos (Murphy, 2018).

[21] Ligação e conexão de vários espaços da internet (Sovrnmarketing, 2010).
[22] Aplicação de partilha de fotos e vídeos na internet (Instagram, s.d).

É através do desenvolvimento de IA que é possível realizar atos de vigilância mais frequentes, abrangentes e constantes sem existir qualquer tipo de limitação a nível de recursos visto que estes atos podem ser desempenhados ou auxiliados por máquinas (McKendrick, 2019). Este ponto é bastante importante visto que os recursos das FSS, infelizmente, demonstram-se limitados.

Esta vigilância desempenhada por ferramentas de IA, para além de permitir uma monitorização constante, permite analisar grandes conjuntos de dados disponíveis através de vários dispositivos em tempo considerado útil para os esforços de prevenção de um ataque, o que à partida, seria impossível para o ser humano. Ganor (2021) explica que quase toda a sociedade, nomeadamente os terroristas, têm uma pegada digital — telemóveis, sistemas de computadores, redes sociais, aplicações, correspondência eletrónica, câmaras digitais, relógios inteligentes — que pode ser monitorizada e processada. Por exemplo, é através da combinação deste conjunto de dados com a utilização de *drones,* que instituições como o exército americano conseguem detetar movimento terrorista, verificar a sua localização e prever a próxima deslocação. No âmbito das redes sociais, está estimado que os terroristas e as suas células publiquem milhares de vezes por dia. Em apenas três meses, o *Computing Research Institute*, no Qatar, analisou mais de três milhões de publicações acabando por detetar apoiantes do Estado Islâmico. Aliás, este algoritmo, através das várias publicações, permitiu identificar quem seriam os apoiantes de uma determinada causa ou quem poderia até vir a ser recrutado para um grupo terrorista com uma precisão de 87% (Ganor, 2021).

Outro exemplo da capacidade de abrangência da IA é o caso de Mike Fikri. Através do *Palantir – software* utilizado por quase todas as agências de segurança dos EUA, que permite às organizações que sistematizem toda a sua informação de uma forma mais eficiente — vários dados que à partida eram insignificantes, depois de decompostos e processados permitiram a prevenção de um ataque terrorista. Fikri, decide viajar do Cairo para Miami ficando hospedado num condomínio. Foram detetados vários levantamentos em dinheiro da sua conta bancária russa e um conjunto de chamadas efetuadas para a Síria. Para além destes dados foi também possível verificar que teria alugado um camião e realizado uma viagem sozinho até à Disney World, em Orlando, tendo passado — (confirmado por testemunhas) , o dia todo a fotografar as zonas com mais multidões. No entanto, durante a sua viagem Mike incorreu numa infração de excesso de velocidade acabando por ser detido e, foi dado um alerta do sistema *Palantir*. Através de uma simples pesquisa foi possível verificar a existência de extensa informação referente a Fikri – impressões digitais, amostras de ADN recolhidas no Cairo, vídeos do suspeito a levantar dinheiro, fotografias da matrícula do camião alugado, registos telefónicos e um mapa que indicava todos os seus movimentos recentes (Ganor, 2020).

Da mesma forma, vários foram os ataques que não foram evitados, mas que poderiam ter sido através do recurso a tecnologias. Em 2011, em Londres no Reino Unido, um conjunto de

hooligans espalharam violência pelas ruas causando mortos e feridos na sequência de uma desordem resultante entre duas claques de futebol rivais, West Ham e Milwall. Maior parte dos elementos apresentavam as caras cobertas, mas os mesmos indivíduos poderiam ter sido identificados através da plataforma *Drop Retrieval*, que permite a análise de elementos de interesse distintos como marcas, tatuagens, cicatrizes e tipos de roupa mais específicos (Mitrea et al., 2015). Ionescu et al. (2020) partilham o exemplo da maratona em Boston, em 2013, onde duas bombas caseiras foram responsáveis por várias mortes e feridos. Neste caso determinadas tecnologias poderiam ter sido usadas para detetar comportamentos estranhos, identificar mochilas ou objetos e identificar alguém que se está a movimentar no sentido contrário da maioria.

Semelhante ao *Palantir*, o SKYNET, é um programa desenvolvido pela Agência Nacional de Segurança dos EUA que, através de IA analisa várias comunicações, sendo possível adquirir um conjunto de informações referentes a possíveis suspeitos de um ataque terrorista (Robins, 2016). Vários estudos têm igualmente sido desenvolvidos, principalmente pela comunidade académica, com o objetivo de criar modelos que possam prever a localização e o tempo de um ataque terrorista (Subrahmanian, 2013) e qual o impacto de determinado fatores, principalmente condições políticas (Choi et al., 2013). Para tal, várias aplicações são utilizadas como base — a aplicação *PredictifyMe*, desenvolvida pelo Estado da Carolina do Norte, em 2014, que, através de 170 pontos de informação, conseguiu prever vários ataques suicidas com 72% de precisão (Lo, 2015); a aplicação *Early Model — Based Event Recognation using Surrogates* (EMBERS) que, através da utilização em conjunto de vários modelos preditivos em separado, permite prever pandemias ou agitação social (Ramakrishnan et al., 2014). Estas aplicações utilizam como fonte redes sociais, páginas referentes a eventos, marcações de restaurantes através da plataforma turística *Booking*, entre outras (Ramakrishnan et al., 2014). No âmbito do combate à radicalização surge o projeto de *Jigsaw — Redirect Method —* que permite determinar a vulnerabilidade de determinado indivíduo em radicalizar-se, identificando utilizadores que partilham vídeos ou fotos que possam ser considerados propaganda extremista (McKendrick, 2019).

Por fim, mas não menos importante, existe um conjunto de projetos a serem desenvolvidos pelo *Institute of Electrical and Electronics Engineers* (IEEE) em Nova Iorque que são merecedores de referência. O *eProfile* permite criar uma área ou perímetro de segurança através da utilização de várias câmaras de vigilância e tem como objetivo responder a cenários críticos e proteger infraestruturas ou zonas de grandes multidões. Esta segurança é realizada através da seleção de pessoas suspeitas através de uma procura de todo o tipo de gravações associadas à mesma, verificando todo o seu comportamento e movimentos prévios. Desta forma, a tecnologia está treinada para reconhecer determinados objetos como malas ou armas e até mesmo eventos de violência como simples empurrões conseguindo assim prever um rápido escalar da violência (Ionescu et al., 2020).

Na vertente áudio, existe o *eTalk,* responsável por gravar todo o tipo de informação quando não existem fontes visuais, ou, existindo, são de má qualidade. Estas gravações são depois transcritas para que um conjunto de palavras chaves sejam detetadas. Este sistema pode ainda, através da voz, criar um perfil de uma pessoa tal como realizar leitura de lábios quando as condições de áudio não são as melhores (Andrei et al., 2019). Devido à existência de um conjunto de informações já adquiridas como dados referentes a escolas, relatórios médicos, viagens, finanças, consumos e comunicações sociais, é possível criar um perfil de determinada pessoa.

O próprio movimento do corpo humano pode ser também estudado e analisado através de *Closed-Circuit Television* (CCTV) (Pugliese, 2008), tal como a postura ou a deteção de objetos nas mãos como sacos ou armas (Greenmeier, 2011). No entanto, vários são os erros apresentados. Na análise da marcha existe sempre a falta de contextualização, ou seja, será que determinada pessoa apenas está triste? E se tiver algum tipo de deficiência motora? Será que tudo isto está a influenciar o seu movimento, não significando necessariamente que esta pessoa irá realizar um ataque terrorista? Visto parte desta observação poder ser desenvolvida por humanos é necessário ter atenção ao fator de subjetividade. Num estudo desenvolvido por Fessler et al. (2012) as pessoas que são vistas a levar uma arma são percecionadas como pessoas mais altas e mais musculadas, mesmo não o sendo, comparadas com pessoas realmente altas e musculadas. Da mesma forma que a mulher e o homem avaliam posturas de formas diferentes (Alaerts et al., 2011).

Por fim, existe o *eSeeming*, utilizado durante entrevistas com possíveis suspeitos, onde câmaras e microfones registam mudanças de humor, expressões e fenómenos de caráter biológico, para detetar algum indicador de mentira (Ionescu et al., 2020). Na área das expressões faciais é importante salientar que autores como Russel (1995) explicam que estão bastante associadas a questões culturais, e que, diferentes expressões podem-se tornar em emoções semelhantes. Contudo, autores como Ekman e Rosenberg (2005) afirmam que os humanos partilham pelo menos algumas expressões faciais universais que identificam emoções comuns. O foco está nas micro expressões e involuntárias, seja de medo, raiva ou de qualquer outra expressão que aparece em microssegundos, independente da tentativa da pessoa de não as mostrar (Ekman, 2003). É de salientar que, muitas pessoas são treinadas para evitar que estas expressões sejam visíveis, mas através da análise de cada *frame* de um vídeo estas podem ser detetadas (Ekman, 1970).

Os sistemas de identificação biométrica permitem recolher e armazenar enormes quantidades de dados sobre características físicas ou comportamentais e traços pessoais, demonstrando ser uma ferramenta preciosa no controlo de acessos, deteção de fraude, documentos de identidade falsificados e identificação de suspeitos de terrorismo (Woodward, 2001). As técnicas são variadas, desde o reconhecimento de impressões digitais, reconhecimento facial, geometria da mão, técnicas de leitura de íris ou retina, reconhecimento de voz e

assinaturas (Woodward, 2001). Porém, é necessária a recolha prévia de amostras de características pessoais de indivíduos e da respetiva representação digital para a criação de modelos que permitirá realizar correspondências entre os indivíduos analisados e os armazenados nos sistemas (Rhodes, 2002). Como tal, o uso de identificação biométrica só é eficaz se existirem informações prévias sobre o indivíduo analisado, caso contrário as decisões irão falhar, seja por incapacidade na identificação, seja por erro (Woodward, 2001). Em todo o caso, estes sistemas são os mais seguros para as autoridades autenticarem identidades devido ao grau de precisão no estabelecimento de correspondências, automatismo ao nível do processamento, conversão imediata dos dados e comparação com bases de dados computadorizados (Liberal, 2012).

Embora em Portugal, no âmbito da segurança humana, a IA não seja uma prioridade, existe um conjunto de países e organizações onde a cultura de segurança está a mudar. Nas Nações Unidas existe um conjunto de laboratórios de pesquisa e desenvolvimento de vários estudos referentes a IA, nomeadamente o United Nations Secretariat's Global Pulse Lab (2021), United Nations High Commissioner for Refugees (UNHCR's), United Nations Office for the Coordination of Humanitarian Affairs (OCHA), o Centre for Humanitarian Data e o Centre for Artificial Intelligence and Robotics pertencente à United Nations Interregional Crime and Justice Research Institute (UNICRI). Foram ainda desenvolvidos o Secretary-General's High-Level Panel on Digital Cooperation (2018) , Secretary-General's Strategy on New Technologies (2018) e o Secretary-General's Report – Our Common Agenda (2021). Estes três últimos projetos têm como objetivo assegurar que todas as pessoas são respeitadas e protegidas na nova era digital e inovar e desenvolver novas ferramentas para a ONU (McCarthy, 2021). Num estudo desenvolvido pela INTERPOL (2021) com o objetivo de verificar os desenvolvimentos na área da IA foi pedido aos vários participantes que partilhassem informações sobre os desenvolvimentos de IA (cf. apêndice A). Foram igualmente discutidos eventuais ferramentas futuras (cf. apêndice B).

2.3. Desafios na utilização de inteligência artificial

Em junho de 2013, Edward Snowden, analista de sistemas, ex-administrador dos sistemas da *Central Intelligence Agency* (CIA) e ex-trabalhador da *National Security Agency* (NSA) dos EUA, denunciou que, através de telemóveis e computadores, as localizações dos utilizadores eram ativadas, vigiando assim os indivíduos e tendo acesso a todo o tipo de informação consultada por eles. Esses dados eram convertidos em algoritmos e inseridos numa base de dados sem qualquer tipo de consentimento (Neiva, 2020). Os temas relacionados com IA e *big data* mudaram para sempre (Van der Vlist, 2017).

De facto, as tecnologias representam grandes benefícios para a sociedade. No entanto, a cada inovação corresponde uma nova vulnerabilidade para a sociedade (Liberal, 2012), sendo apenas possível avaliar os riscos com maior exatidão nos próximos anos (Fernandes, 2020).

De uma forma geral existem três tipos de argumentos em relação aos vários medos associados ao uso de IA, a saber — o genérico, o utilitarista e o ético (Ganor, 2021). O primeiro, retrata as preocupações normais sobre o exponencial desenvolvimento da IA e todo o impacto que pode ter na sociedade; o segundo afirma que é impossível utilizar a IA como forma de combate ao terrorismo; os argumentos éticos englobam os possíveis danos em cidadãos inocentes, sendo que para o combate ao terrorismo em específico esta tecnologia não deve ser usada (Ganor, 2021).

Um dos principais medos é que a IA alcance resultados ou funções que os seus programadores não permitiam inicialmente. Nesta linha de pensamento, existe o medo de que, tal como o cérebro humano tem uma capacidade de aprendizagem através da tentativa-erro, uma máquina possa vir a conseguir fazer o mesmo, mas de uma forma mais rápida e sem qualquer valor ético-moral para balizar essa ação. Mesmo na gestão de recursos, uma máquina pode não ter os mesmos critérios de um humano (Ganor, 2021).

Relativamente à utilização de IA para combater o terrorismo, autores como Munk (2017) questionam se os ataques terroristas podem realmente ser evitados. Este autor explica que a IA é responsável por bastante erros teóricos que a mínima tentativa de prevenção é ineficaz, arriscada e inapropriada visto existir o risco, por mais mínimo que seja, de sinalizar erradamente como suspeitos cerca de 100 000 pessoas inocentes, visto que, (1) o terrorismo é um evento irregular que acontece poucas vezes e que facilmente pode ser confundido; (2) cada ataque é único e através de uma pequena base de dados podem surgir generalizações incorretas; (3) não existe uma única definição sobre o que deve ser considerado uma tentativa de ataque terrorista e, ataques falhados não são na sua maioria conhecidos; (4) não existe consenso sobre o perfil do terrorista, não existe igualmente um perfil que se encaixe em todas as organizações existentes, nem sequer um único perfil dentro da mesma organização; (5) não existe a certeza de quando e como uma pessoa com ideias extremistas pode vir a realizar ações violentas, ou seja, a diferença entre um potencial terrorista e um terrorista real não está definida, podendo vir a causar erro na identificação destes; (6) o terrorismo é um fenómeno dinâmico que está constantemente a evoluir, ou seja, características que são agora utilizadas para definir terrorismo podem amanhã já não o ser, tornando-se as mesmas irrelevantes (Munk, 2017). Existe ainda a possibilidade de existir uma falha ao detetar um ataque, ou seja, um “falso positivo” — o sistema descarta um sujeito como não terrorista, mas este tem uma bomba e acaba por embarcar num avião (Ganor, 2021).

Para além destas possíveis falhas, os sistemas biométricos de reconhecimento facial têm sido um assunto controverso em relação à sua utilização. Cumpre ainda referir que estes sistemas têm apresentado erros na identificação de refugiados, demonstrando ser menos precisos na identificação de mulheres e de pessoas de cor (Boulamwini & Gebru, 2018). Ao contrário do ser humano que tem uma grande capacidade de adaptação, pesquisas mostram que basta uma

pequena mudança numa imagem para alterar a forma como a realidade é percecionada por máquinas de reconhecimento (Hosseini, 2017), ou seja, se existir o desejo de tentar mudar ou enganar uma aplicação de reconhecimento de imagem, há formas efetivas de o fazer, visto que é impossível supervisionar a atuação das máquinas constantemente (Goodfellow et al., 2017). Existe ainda um conjunto de limitações técnicas, ou seja, independentemente do grau de sofisticação da IA e da quantidade de dados disponíveis, prever o terrorismo e a radicalização poderá ser algo bastante difícil.

Passando para um conjunto de receios mais abrangentes, mas não menos importantes, verificamos o sentimento de falta de controlo e de regulamentação, que, caso não existam, a vertente mais legal será ignorada, diminuindo assim a transparência de determinadas instituições acabando por enfraquecer o seu poder de decisão (Dechesne et al., 2016). Um exemplo desta falta de controlo é a crescente expansão de IA a ser utilizada pelo setor privado. De acordo com Cagle (2016) muitas companhias privadas obtêm informação sobre o público acabando por as vender mais tarde às FSS, ou seja, o Estado obtêm informação que não consegue obter através de meios legais. A maior parte dos dados provêm de pessoas que não são do interesse dos serviços de inteligência, o que acaba por causar inquietação, fazendo com que o critério da proporcionalidade seja posto em causa, visto que mesmo a informação não sensível pode colocar em causa o direito à privacidade (McKendrick, 2019). Nesta linha de pensamento, surge também o receio de que informação e dados que são recolhidos para inicialmente serem utilizados para o combate ao terrorismo acabem por ser utilizados para combater outros crimes — O New York City Police Department's Domain Awareness System tem cerca de 3 000 CCTV que inicialmente foram instaladas para combater o terrorismo, mas os objetivos têm sido outros (Levine et al., 2017). A informação deveria ser apenas analisada por um conjunto de analistas tornando assim todo este processo mais sigiloso. Consequentemente surge também o risco de intrusão ou roubo de informação confidencial ou reservada (Oliveira, 2021).

Os limites no acesso a informação tem consequências nos receios aqui apresentados. De acordo com Ganor (2021), quanto mais informação existir, maior será a qualidade dos modelos de previsão. Com as restrições sobre os dados que podem ser acedidos, a legitimidade das decisões tomadas com base nesses mesmos poderá ser reduzida, podendo estas decisões não ser as mais corretas visto os dados utilizados não serem representativos nem de qualidade. No entanto, devemos salientar que o total acesso a informação não significa de todo o sucesso a criação de modelos preditivos fiáveis, é também necessário que estes sejam validados e testados (O'Neil, 2016). Desenvolver estes modelos de uma forma cientificamente objetiva é bastante difícil, visto que na sua elaboração entram vários fatores subjetivos, como por exemplo fatores culturais — presunções baseadas em viagens para determinados países e diferentes tratamentos de determinados grupos sociais (Larson et al., 2016). No âmbito policial, estas decisões podem retratar visões discriminatórias ou racistas, tornando-se as respostas difíceis de explicar devido

à opacidade dos dados (Fernandes, 2020). Em suma, os que vigiam tornam-se mais omnipresentes mas ocultos perante os vigiados (Costa, 2004) e os vigiados tornam-se mais transparentes (Ferreira, 2014).

O medo clássico de a sociedade ficar totalmente dependente das máquinas e da IA sempre existiu e continuará a existir. Kissinger (2018) afirma que esta dependência poderá contribuir para um retrocesso da sociedade, onde deveria existir uma dependência pelas normas filosóficas e éticas e não por meros instrumentos. A crescente disponibilidade de dados pode levar a uma erosão das normas sociais na medida em que, devido a esta violação de direitos, qualquer intervenção policial passaria a ser aceite, tornando-se legítima só porque uma simples máquina disse que assim deveria ser, passando a tolerância ao risco e à incerteza a ser menor (Hert & Lammerant, 2017).

Nesta linha de pensamento é muitas vezes discutido a legitimidade para atuar tendo em conta uma possível previsão do futuro, ou seja, ao desenvolver novas tecnologias preditivas estará a ser criado conhecimento sobre o futuro, assim as autoridades estarão a punir e intervir antes de um crime acontecer (Puyvelde et al., 2017). A partir de vários estudos para analisar a forma como a existência de uma vigilância digital generalizada poderia influenciar o comportamento da sociedade, rapidamente se conclui que tal pode gerar alguma ansiedade devido a meras opiniões ou críticas políticas. Só o simples facto de uma pessoa saber que está a ser observada faz com que o seu comportamento se altere drasticamente (Goldman, 2014) — uma coisa é a mera observação pelos nossos pares, outra é a observação pelo governo (Townsend, 2014). O facto de os assuntos securitários serem, na sua maioria, da responsabilidade do Estado gera algumas inseguranças porque mesmo que existam regulamentações e limitações, existe medo do abuso de autoridade (McKendrick, 2019). É percetível que o direito tem dificuldade em acompanhar a inovação tecnológica (Neiva, 2020). No âmbito da própria investigação criminal, a Europa prevê através da Diretiva 2016/680 a proteção de dados no contexto de *big data*, mas existe um vazio legal sobre a forma como os polícias devem fazer uma análise dos algoritmos e tomar decisões (Neiva, 2020).

Para além da capacidade de reconhecimento de um sistema de IA poder ser afetada por condições de iluminação (Comissão Europeia, 2020b), determinados algoritmos de IA, quando utilizados para prever a reincidência criminal podem retratar preconceitos (Tolan et al., 2019). Surge a necessidade de requisitos específicos para os riscos possíveis, bem como outros mecanismos destinados a assegurar a manutenção da qualidade dos dados ao longo dos tempos (Comissão Europeia, 2020a). Uma decisão humana não é imune a erros e objetiva, mas uma má decisão de um sistema de IA pode ter um efeito muito maior, afetando e discriminado pessoas sem os mecanismos de controlo social que regem o comportamento humano (Comissão Europeia, 2020b).

Os produtos de IA apresentam vários níveis de opacidade fazendo variar a compreensão do processo de tomada de decisão do sistema (o chamado «efeito de caixa negra»). À medida que os algoritmos de IA tornam-se mais avançados e inteligentes, principalmente em áreas críticas como a da segurança, é imperativo perceber o motivo de determinadas decisões (Comissão Europeia, 2020a). Consequentemente surge outro grande risco: quem deve assumir a responsabilidade no caso de um erro? Quem implementou, criou ou confiou na decisão? Neste caso torna-se extremamente difícil reunir os elementos de prova necessários para instruir um processo em tribunal, bem como o preenchimento de condições para pedido de uma indemnização (Comissão Europeia, 2020a). É importante garantir que as vítimas destes acidentes não beneficiem de um nível de proteção inferior ao das vítimas de acidentes relacionados com outros produtos ou serviços semelhantes. De certa forma, a contratação de seguros poderiam prevenir algumas das consequências negativas dos acidentes através da existência de regras claras (Comissão Europeia, 2020b).

A temática da IA apresenta um dilema pois na prevenção do terrorismo, em particular, mas de uma forma geral nos serviços inteligência, existe uma forte necessidade de preservar determinados valores e direitos individuais. No entanto, muitas vezes estes entram em conflito com a necessidade de proteger a vida humana. Se existe a possibilidade de a IA detetar um terrorista porquê tanta hesitação? O funcionamento da IA não é fácil de entender, não é simples explicar como é que o terrorista X foi detetado, criando uma ideia de que qualquer um de nós poderia, injustamente, ter sido escolhido (Yoelle, 2018).

2.4. Possíveis soluções para os desafios da inteligência artificial

Os contributos para os dilemas e desafios anteriormente apresentados são vários.

O *Office for the Coordination of Humanitarian Affairs* (OCHA) desenvolveu um manual que especifica todas as fases na revisão de pares dos vários sistemas de IA que podem vir a ser implementados (OCHA, 2021). O objetivo é criar um método de revisão por especialistas, quer na área de gestão de dados, tecnologia e estatística, quer na área da ética prática e humanitária, gerando assim uma validação científica.

A UNESCO tem promovido encontros intergovernamentais desde 2019 para articular recomendações relacionadas com ética na utilização de IA, tendo sido criado em 2020 um projeto de regulamento internacional onde valores como a transparência, a igualdade de género e os direitos humanos são o foco principal. Este novo documento estaria alinhado com outros já existentes das Nações Unidas como a Declaração Universal dos Direitos Humanos (DUDH) e a Convenção dos Direitos da Criança (CDC). O objetivo é que este documento seja mais do que uma mera recomendação e que possa ser voluntariamente retificada pelos Estados Membros, comprometendo-se com os princípios estipulados em cada jurisdição (OCHA, 2021).

Para uma correta regulamentação da IA, a Comissão Europeia propõe uma abordagem baseada em quatro níveis (inaceitável, elevado, limitado e mínimo) definidos de acordo com a finalidade de uso, pessoas afetadas, irreversibilidade de danos e medidas para minimizar riscos. Esta regulamentação é aplicada aos fornecedores que coloquem no mercado ou em serviço sistemas de IA no território da União, estejam ou não estabelecidos na União ou país terceiros; a utilizadores de sistemas de IA localizados na União; a fornecedores e utilizadores de sistemas de IA localizados em país terceiro, se o resultado produzido pelo sistema for utilizado na União. No primeiro nível enquadram-se utilizações particularmente nocivas que violam os valores definidos pela UE no campo dos direitos fundamentais como por exemplo, exploração de vulnerabilidades nas crianças, uso de técnicas subliminares e sistemas de identificação biométrica à distância em tempo real. De seguida, no patamar do risco elevado, estão todos os sistemas que afetam negativamente a segurança dos cidadãos, sendo necessário o cumprimento de determinados requisitos como a qualidade dos dados, disponibilidade de documentação técnica e conservação de registos, transparência e supervisão humana, devendo ser avaliados por organismos independentes. Dentro do risco limitado, os requisitos são ainda mais específicos, principalmente no campo da transparência, por exemplo, sempre que existir um pequeno risco de manipulação de informação ou dados, todos os seus utilizadores devem estar cientes desse facto. Por fim, é no risco mínimo que se enquadra a maior parte dos sistemas utilizados pela EU sendo que devem respeitar a legislação em vigor sem qualquer outro tipo de obrigação jurídica adicional. Existe um conjunto de sistemas que estão expressamente proibidos - sistemas que possam levar à classificação social de determinadas pessoas, contribuindo para fatores de exclusão social ou discriminatórios, sistemas que distorcem comportamentos, que provoquem danos físicos ou psicológicos e a utilização de componentes subliminares não detetadas por humanos. Embora estes sistemas sejam proibidos, tal não significa que não possam ser investigados para efeitos legítimos porém, essa investigação não pode criar danos para os cidadãos, devendo ser desenvolvida de acordo as normas éticas previamente já definidas (Comissão Europeia, 2021).

É necessário incentivar o debate sobre o impacto destas tecnologias nos direitos fundamentais para que a segurança dos utilizadores seja garantida e respeitada, aumentando consequentemente, a confiança na IA, não só dos cidadãos mas principalmente das empresas. De modo a garantir o cumprimento das várias regulamentações em desenvolvimento, cada Estado-membro da UE deve nomear uma ou várias autoridades nacionais competentes para supervisionar a aplicação e execução de atividades de fiscalização do mercado. Existe ainda um Comité Europeu para a IA composto por representantes de alto nível das autoridades nacionais de controlo competentes, da Autoridade Europeia para a Proteção de Dados e da Comissão da presente regulamentação. O seu objetivo é permitir uma aplicação mais harmonizada do novo regulamento da IA, podendo também emitir recomendações ou pareceres, contribuindo assim para o acumular de conhecimento especializado sobre a área.

É pertinente analisar várias dúvidas referentes ao uso da identificação biométrica. Existe uma grande dificuldade em criar uma definição consensual daquilo que é assumido como "espaço acessível ao público", visto que estes sistemas apenas devem ser usados nestes espaços. Por espaço acessível ao público, entende-se todo o espaço físico que seja acessível ao público, independentemente do espaço em questão ser detido por uma entidade privada ou pública, logo, esta definição não abrange espaços privados que não são de livre acesso de terceiros, incluindo de autoridades policias, a não ser que tenham sido especialmente convidados ou autorizados. Espaços como ruas, partes relevantes de edifícios governamentais, infraestruturas de transportes, cinemas, teatros, lojas e centros comerciais são, à partida, acessíveis ao público. No entanto, esta definição não é linear. Para verificar se um espaço é acessível ao público deve recorrer-se a uma análise casuística tendo em conta as especificidades de cada situação (Parlamento e Conselho Europeu, 2021). Estes sistemas de identificação biométrica são considerados de risco elevado, e, mesmo que utilizados para efeitos de ordem pública, o seu uso é considerado particularmente intrusivo visto direitos fundamentais como a dignidade humana, respeito pela vida privada e familiar, proteção de dados pessoais poderem ser violados, contribuindo igualmente para uma sensação de vigilância constante. Visto existir sempre um risco de falha de exatidão nos seus resultados, tendo em conta que os mesmos dependem de um conjunto de fatores como a qualidade da câmara, iluminação, distância, base de dados existentes, é imprescindível que sistemas como estes estejam constantemente a serem adaptados, testados e discutidos de modo a evitar resultados discriminatórios. Os atuais sistemas diminuíram drasticamente a sua taxa de falsos positivos, passando a operar com uma exatidão de 99%. No entanto, mesmo quando a percentagem de erro é apenas 0,1% num universo de dezenas de milhares de pessoas, o risco é bastante elevado. Para fins policiais, a utilização deste sistema faz parte de uma das raras exceções estritamente definidas e limitadas - busca direcionada para potenciais vítimas específicas de crimes como crianças desaparecidas; resposta a um possível ataque terrorista e identificação e deteção de autores de crimes graves (art 16.º TFUE e art 10º da Diretiva EU 2016/680). Para a utilização destes sistemas, os mesmos devem estar sujeitos a autorizações expressas e específicas de uma autoridade judiciária ou uma autoridade administrativa independente de um Estado-Membro. Esta deve ser obtida antes da utilização, salvo em situações de urgência devidamente justificadas, sendo que nestas situações deve limitar-se ao mínimo absolutamente necessário de utilização. O próprio Estado lesado e onde será utilizado o sistema deve também autorizar o mesmo (Parlamento e Conselho Europeu, 2021).

No que diz respeito ao armazenamento de dados, o ideal era existir uma centralização, ou seja, os vários resultados de análise conduzidos por diferentes agências, privadas ou públicas, estariam sobre o mesmo regime de regulação e sistema de análise. Automaticamente, as atividades seriam mais fáceis de regular tal como acabaria por melhorar a capacidade de

direcionar recursos de uma forma mais eficiente (McKendrick, 2019). Poderiam ser ainda concedidos direitos mais amplos de acesso aos dados pelos serviços de inteligência para efeitos de análise automatizada visto que esta é menos intrusiva do que a análise humana (Roettgers, 2017). De acordo com o mesmo autor, quando um grande conjunto de dados é recolhido, na análise automatizada, o que não interessa é rapidamente eliminado e não é armazenado para ser posteriormente consultado por humanos para verificarem o que vale ou não a pena analisar. Como possível solução à carga subjetiva proveniente da supervisão humana surge a aposta em modelos de IA com base em métodos quantitativos, que permite comprovar a sua eficácia, garantindo que o objetivo é legítimo e proporcional reduzindo assim uma possível discriminação (Hardt et al., 2016). É através de uma base quantitativa que é possível distinguir um modelo preditivo de um modelo que apenas tem como finalidade a busca de mera informação (Hert & Lammerant, 2017).

Em suma, é o desconhecido que inquieta a sociedade, o não perceber como foi feita determinada escolha. Como tal, explicar os modelos e partilhar o processo de decisão dos mecanismos de IA poderá fazer com que o público não veja estas medidas como simplesmente discriminatórias. Esta troca de informação não só aumentava a confiança que o cidadão tem nas FSS como também a partilha entre atores internacionais e outras agências de segurança (McKendrick, 2019).

2.5. Inteligência artificial e o meio policial

De uma forma geral, a polícia já utiliza IA em várias atividades (dependendo dos países), nomeadamente, — na prevenção do crime, manutenção da ordem e segurança pública, investigação criminal, segurança pessoal, gestão dos registos policias, planeamento operacional, automatização de tarefas repetitivas, atendimento digital, reconhecimento automático de matrículas, reconhecimento facial e identificação de vítimas (Rademacher, 2020).

O trabalho policial com IA é baseado em quatro áreas: (1) prevenção e análise através de grandes quantidades de dados; (2) reconhecimento com câmaras ao vivo e reconhecimento de voz; (3) exploração com veículos autónomos para patrulha; (4) comunicação (UNICRI, 2021). Fernandes (2020) acrescenta ainda que a IA pode ser utilizada para prevenção criminal, nomeadamente previsão de ocorrências de crimes, de indivíduos em risco de cometer crimes, para identificação de suspeitos e de eventuais vítimas.

De referir a existência do European Dactyloscopy (EURODAC), o mais antigo banco de dados biométrico europeu de larga escala a operar desde 2003, cuja função consiste em recolher e processar impressões digitais de requerentes de asilo, de pessoas que atravessam a fronteira irregularmente e daqueles que se encontram ilegalmente em território da UE (Neiva, 2020).

Determinadas polícias acabam por se destacar, nomeadamente a polícia dos Países Baixos (Custers, 2012) — apenas em 2016 cerca de 130 projetos tecnológicos foram desenvolvidos pela polícia nacional dos Países Baixos (Ernst & Kop, 2018).

Os Países Baixos preferem adotar uma abordagem bastante ampla, abordando não apenas os atos de violência em si, mas também a cadeia de eventos que os precede, ou seja, o objetivo é a prevenção, intervir o mais cedo possível, de preferência durante o processo de radicalização, evitando assim medidas repressivas. As suas medidas preventivas no âmbito do combate à radicalização têm como objetivo criar condições para a participação social garantindo que os grupos mais vulneráveis possam usufruir dos benefícios da sociedade. Este objetivo é garantido através de (1) reforços dos laços sociais e civis já existentes na sociedade principalmente através do combate à discriminação no mercado de trabalho; (2) promoção de uma cultura de entendimento através do desporto; (3) melhorar o conhecimento dos jovens sobre o Islão; (4) prevenir o isolamento, polarização e radicalização através da reintegração de indivíduos que podem pôr em causa a sociedade e a democracia; (5) identificar os casos de radicalização o mais cedo possível; e (6) limitar a influência de pessoas extremistas na sociedade. Já nas medidas repressivas o foco está em eliminar todo o conteúdo que possa transmitir ódio ou propaganda terrorista (Committee of experts on terrorism, 2008). Todos estes objetivos são auxiliados por mecanismos ou sistemas de IA.

Na investigação de Brayne (2017), durante dois anos e meio no Los Angeles Police Department (LAPD), foi possível confirmar que através de uma análise de grande número de dados, as práticas de vigilância tornavam-se mais fáceis, permitindo que a atuação policial fosse mais preventiva. É através destes dados que o *software* OPERAÇÃO LASER (Los Angeles Strategic Extraction and Restoration Program) relaciona lugares e indivíduos potencialmente perigosos, contribuindo assim para a redução das taxas de criminalidade. A cada indivíduo está associado um Certificado de Registo Criminal ao qual é dada uma cotação proporcional à gravidade do ato cometido. De seguida, são elaborados índices ordenando os indivíduos para depois serem partilhados pelos diferentes Departamentos e Setores da Agência Policial (Brayne, 2017).

Numa altura em que o policiamento depende cada vez mais de *softwares* e recolha de grandes conjuntos de informações, é urgente entender o potencial destas tecnologias. Este é o ponto de vista da polícia francesa explorado por Kubler (2017). Desde 2005, esta polícia usa o IBM's Computer Program: i2 Analyst's Notebook[23] — para agregar informações e criar narrativas criminais. Através dos vários dados disponíveis (suspeitos, locais, objetos, vítimas), o sistema

[23] É uma tecnologia utilizada há 20 anos por mais de 2.000 organizações por todo o mundo. Foi criada para auxiliar as instituições do governo e empresas privadas na luta contra o terrorismo e organizações criminosas. Esta fornece uma grande capacidade de análise visual através de um conjunto de dados e informações complexas permitindo que os analistas identifiquem e consigam prevenir o crime (IBM Corporation 2017).

realiza várias conexões entre estes encontrando associações anteriormente não adquiridas, priorizando assim o nível de importância desses dados para uma investigação (Kubler, 2017).

Na Austrália foram conduzidas entrevistas a 38 funcionários responsáveis pela aplicação da lei, desde agentes policiais, legisladores, informáticos até membros da sociedade civil (Chan & Moses, 2015). De uma forma geral, na sua maioria, todos concordavam que o *big data* era de facto inovador e que criava oportunidades para prevenir a criminalidade, porém, poucos sabiam realmente o que era o *big data*. Aliás, os próprios polícias confessavam não ter tempo nem recursos para beneficiar desse mesmo potencial (Chan & Moses, 2015).

Por fim, no que diz respeito à Europol, Drewer e Miladinova (2017) reconhecem que em áreas como o terrorismo, o *big data* pode ser bastante útil, permitindo a criação de perfis mais rapidamente. É urgente a criação de um modelo proativo ágil e adaptável que seja criado através das novas tecnologias existentes. Aliás, a Europol prevê o desenvolvimento de uma tecnologia inovadora que irá conectar 500 agências policiais na Europa utilizando os seus bancos de dados e oferecendo recursos rápidos e seguros com respeito pela privacidade, proteção e segurança dos dados (Drewer & Miladinova, 2017).

Num estudo desenvolvido pelo National Institute of Justice (NIJ), dos EUA, que abrangeu quatros FSS com mais de 1000 elementos cada um e com jurisdições quer em áreas urbanas, quer a áreas mais rurais, foi possível concluir que existem cerca de nove fatores que influenciam a forma como a tecnologia é incorporada, que se destacam infra:

(1) a experiência da própria organização com a inovação tecnológica - Quais as razões para determinada tecnologia ter sido escolhida? Quem esteve envolvido no processo de implementação? quais os maiores desafios nesta implementação? Quais os resultados?;

(2) a cultura policial - É algo positivo para os polícias? A tecnologia responde positivamente às necessidades policiais? Esta altera a forma do trabalho policial?;

(3) as unidades organizacionais, hierarquia e estrutura — A IA aumenta ou diminui a comunicação entre as várias hierarquias? Cria uma maior sensação de igualdade? Facilita o trabalho em grupo? Cria um melhor ambiente?;

(4) a responsabilidade interna e gestão de sistemas — De que forma as tecnologias contribuem para o aumento ou diminuição da responsabilidade?

(5) o polícia individual, discrição e processo de decisão — Que tipo de tarefas são desempenhadas com as tecnologias? A discrição é aumentada ou diminuída? A tecnologia é útil?;

(6) a eficiência do processo policial e produtividade diária — Como a tecnologia pode tornar o trabalho policial mais eficiente e produtivo? Como mudou as suas atividades?;

(7) a eficácia em reduzir o crime — Surgem mudanças na forma como o crime é abordado? É possível medir os impactos da tecnologia para medir os esforços da policia a reduzir o crime?;

(8) a comunicação entre polícia e cidadão e legitimidade policial — Existem direitos a ser violados? O cidadão sente-se mais seguro?;

(9) a satisfação laboral — A tecnologia torna os polícias mais criativos e inovadores na resolução de ocorrências? Reduz a sua satisfação? Cria stress? Reduz a sua autonomia e discrição?.

O impacto da IA na cultura policial não é indiferente. A forma como a tecnologia foi recebida pelas FSS foi influenciada por crenças já existentes sobre experiências passadas. Muitos afirmavam que a integração da tecnologia era um processo bastante demorado e que os programas não eram sofisticados. Porém, outras unidades com experiências positivas retratavam com confiança que a tecnologia contribuía para um trabalho mais fácil e eficaz.

O próprio *design* da tecnologia é um ponto fundamental. Quanto mais *user friendly*[56] for uma tecnologia, mais fácil será de trabalhar, não se tornando uma tarefa difícil e cansativa.

A forma de liderança pelas chefias é considerado um dos principais fatores para uma boa receção das tecnologias – numa unidade em específico as chefias demonstram preocupação e cuidado acrescido em transmitir uma mensagem clara relativamente ao funcionamento das tecnologias, tal como também tentaram adaptar os objetivos, quer dos polícias como o das tecnologias, de modo a que estes ficassem alinhados. Consequentemente, as tecnologias foram recebidas com outro tipo de expectativas, ao contrário de outra unidade onde não foi realizada qualquer reunião, exercício de comunicação ou esclarecimento, polícias como os pertencentes à patrulha acabaram por se sentir injustiçados ou incompreendidos visto não existir qualquer planeamento ou apoio técnico.

Por fim, concluiu-se que o fator idade e geracional foi bastante decisivo. Invariavelmente, os elementos mais jovens demonstravam mais entusiasmo com a IA comparado com os elementos mais antigos. Os primeiros sentiam-se curiosos e esperançosos referentes às possíveis mudanças que a IA poderia trazer para o seu trabalho, já os mais velhos demonstraram um pouco de resistência, sentindo que o seu trabalho não iria ser útil, acabando por demonstrar sentimentos de frustração e desmotivação.

As novas tecnologias influenciam o próprio funcionamento da organização, da estrutura e até mesmo da hierarquia da força policial, reajustando assim várias estruturas organizacionais e relações existentes. Em determinadas unidades houve uma preocupação com a existência de uma integração correta das tecnologias, como tal, foram desenvolvidas novas unidades ou subsecções para ajudar os elementos a trabalhar com as tecnologias. No entanto, muitos oficiais acabaram por partilhar que não conseguiam estar na rua tanto como desejavam, aumentando mais o seu trabalho administrativo e indicando que, aos poucos deixavam de ser líderes, passando a ser meros gestores de humanos e máquinas. Relativamente à comunicação, devido à necessidade constante de esclarecimento de dúvidas, houve um aumento significativo de

comunicação e troca de ideias, nos casos em que não houve qualquer tipo de apoio, a comunicação não sofreu alteração.

No exercício da responsabilidade interna, a mudança foi sentida tanto pelas chefias, como pelos polícias menos graduados, aumentando principalmente o controlo dos primeiros. Se, por um lado, os oficiais conseguem monitorizar a atividade dos seus elementos e gerir melhor os seus recursos, os elementos da patrulha que sempre tiveram bastante autonomia, passam a sentir uma maior pressão, visto existirem tecnologias constantemente a registar todo o seu trabalho onde tudo está visível aos olhos de todos. Assim, estes acreditam que a sua discrição no âmbito profissional é também limitada — por exemplo, no âmbito de uma ação de proximidade e visibilidade, em vez de estes escolherem a zona mais adequada para o efeito, têm de escolher uma zona onde exista rede ou dados móveis, podendo este local não ser o melhor para o objetivo inicial. É interessante observar como muitas chefias afirmam que a tecnologia em si nunca irá incentivar ou aumentar a proatividade. Todavia, a responsabilidade não é da tecnologia *per si*, mas sim da própria cultura policial onde os polícias, de uma forma geral, só são proativos se estiverem insatisfeitos ou entediados durante o seu turno ou se estiverem pessoalmente motivados.

Relativamente à satisfação com o trabalho as respostas são mais complexas. Quando é feita uma detenção, ou determinado caso policial é resolvido através do uso da tecnologia, os polícias ficam extremamente motivados, acabando por desejar aprender mais sobre a tecnologia de modo a que consigam retirar o máximo potencial da mesma, para que situações como as primeiras se voltem a repetir. No entanto, os polícias afirmam que a sua satisfação com o trabalho em nada tem que ver com tecnologias, antes com aspetos organizacionais que possam estar associados às tecnologias como as chefias, processos de liderança e planeamento antecipado.

De acordo com o estudo em análise referente às relações com a população, as respostas foram variadas. Em certos casos houve uma exponencial melhoria, através de aplicações *user friendly*, permitindo à população estar mais próxima da polícia, conhecer as suas rotinas, o seu trabalho, histórias de sucesso e esclarecer dúvidas. No entanto, em determinados casos, os polícias comentavam que deixavam de ter tempo para andar na rua e criar ligações mais fortes com o cidadão, principalmente com os mais vulneráveis. Quando questionada a população, mesmo tendo em conta o ponto positivo apresentado primeiramente, muitos partilhavam que não gostavam de se sentir constantemente observados por determinadas tecnologias, expondo receios já apresentados nos capítulos anteriores referentes ao grande medo de, um dia, as tecnologias virem a substituir os humanos.

Depois de explorados os vários pontos que contribuem para uma boa ou má implementação das tecnologias, o estudo desenvolvido pelo NIJ acaba por sugerir recomendações para que as tecnologias possam ser bem rececionadas, tornarem-se benéficas para o trabalho policial e reduzirem os riscos e medos associados. Desta forma, é importante construir e ajustar as normas

organizacionais antes da adoção da tecnologia. Por exemplo, é necessário que cada unidade policial estabeleça as suas prioridades, objetivos e estratégias. Se os objetivos são apenas realizar o máximo de detenções e apreensões possíveis, então determinada tecnologia pode não ser a mais indicada, tal como se o objetivo for de prevenção com resultados a longo prazo. Aliás, neste caso é sugerido que as esquadras realizem primeiro um conjunto de testes para verificar se determinada tecnologia é adequada para os seus objetivos. No entanto, é de salientar que, os efeitos da presença de tecnologia nas forças de segurança é mais visível a longo prazo.

Não só para obtenção de bons resultados, mas também para uma maior satisfação laboral, é necessário que exista um treino constante, uma melhoraria dos papéis funcionais que todos devem desempenhar nas esquadras contribuindo assim para melhores expectativas e reforço da cultura policial.

No âmbito da formação ou criação de planos de formação, a elaboração destes planos não pode ser apenas realizada pelas altas chefias sendo que muitas delas poderão nem vir a ter qualquer contacto com as tecnologias. O ideal é que todas as pessoas que serão afetadas ou estarão envolvidas possam participar no processo de adesão, planeamento e implementação de modo a esclarecer todas as dúvidas que possam surgir ou até mesmo a ajudar a especificar em que áreas determinada ferramenta pode ser útil. Consequentemente, a polícia deve fazer parte do desenvolvimento do *design* e da criação da própria ferramenta, ou seja, uma tecnologia que é desenvolvida para objetivos policiais será bastante diferente de uma que é desenvolvida para uma empresa. Desta forma questões de segurança, éticas e valores e até prática necessária para o trabalho operacional serão garantidas. Em caso negativo, estas ferramentas estarão apenas a contribuir para o desperdício financeiro, más associações e desmotivação (Koper et al., 2015).

Capítulo III. Método

3.1. Considerações metodológicas

Uma investigação académica deve ser elaborada através de métodos específicos de acordo com o objeto de estudo produzindo assim conhecimento válido, verdadeiro e científico e permitindo ao investigador uma tomada de decisão mais segura referente ao problema de investigação. O método são as várias atividades que permitem alcançar o(os) objetivo(os) previamente estabelecidos com maior segurança e eficácia (Marconi & Lakatos, 2017).

Desta forma, ao longo do processo do método científico de Creswell e Poth (2018) é possível observar cinco grandes fases: a constituição do problema, a elaboração de hipóteses ou questões, a recolha de dados, os resultados e, por fim, a discussão.

Numa primeira fase, foi desenvolvido o estado da arte através da pesquisa e análise de bibliografia existente, de modo a retirar todos os dados e factos relacionados com o tema que fossem atuais e relevantes (Marconi & Lakatos, 2017). A literatura consultada é maioritariamente produzida em países europeus e nos EUA (ainda pouco explorada em Portugal) e consistiu quer em livros e capítulos de livros, quer em artigos científicos, referências jornalísticas, monografias e documentação institucional ou governamental, maioritariamente, de caráter internacional.

Sob a ótica de Quivy e Campenhoudt (2008), a formulação da pergunta de investigação deve atender a diversos aspetos, nomeadamente clareza, pertinência e exequibilidade, para que seja possível obter dados ou informações que possam responder ao problema em questão. Para a produção de um estudo coeso e sólido, é necessário que a pergunta de investigação, os vários objetivos e o método estejam alinhados e interconectados (Creswell & Poth, 2018). Recorrendo à literatura estudada e exposta ao longo da presente dissertação, percebe-se que o crime de terrorismo está em constante mutação e que se foi adaptando a esta grande revolução tecnológica e comunicacional na sociedade, tornando-se mais difícil de combater. Urge encontrar novas medidas de contra terrorismo, logo, é vital perceber se o uso de IA poderá ser uma delas, respondendo assim à seguinte pergunta de investigação: qual o papel da IA no combate ao terrorismo em Portugal?

Uma vez que o pretendido é direcionar o foco para um conjunto de dados e, simultaneamente, assimilar várias perceções ao longo do processo de recolha de dados, foi selecionada uma abordagem qualitativa (Neuman, 2014), pois permite enfatizar as palavras na recolha e análise de dados ao invés de as quantificar (Bryman, 2012).

Tendo em conta que a IA é uma temática em desenvolvimento, os elementos de flexibilidade e abertura, característicos das abordagens qualitativas, foram decisivos na escolha deste método (Creswell & Poth, 2018, p. 111). Após a identificação de um problema, a investigação tem como objetivo desenvolver conhecimento através de várias hipóteses conceptuais baseadas em conceitos e vários paradigmas atuais (Sarmento, 2013), neste caso em específico, não foram

elaboradas hipóteses, mas sim questões de investigação de modo a obter respostas que permitissem contribuir para o aumento de conhecimento na área do uso da IA no combate ao terrorismo.

Em suma, a escolha de um estudo exploratório para nortear o presente trabalho foi o mais indicado para examinar este fenómeno ainda pouco explorado e permitir organizar de forma pertinente conteúdo para futuras investigações (Neuman, 2014).

3.2. Participantes

A seleção inicial de participantes baseou-se na necessidade de recolher informação especializada quer em terrorismo, quer em IA. No entanto, visto o número de participantes com conhecimento nestas duas áreas em conjunto ser reduzido, foi necessário alargar o leque a outros participantes especialistas numa daquelas vertentes.

Atento ao caráter exploratório da dissertação, um dos principais objetivos na abordagem da IA no combate ao terrorismo foi obter uma perspetiva mais estratégica e ampla e não tanto tática ou operacional. Desta forma, da carreira policial, foram apenas selecionados aqueles que pertencem à carreira de Oficial de Polícia. Participaram assim neste estudo um Oficial de Polícia com vasta experiência na área do terrorismo, das informações e da *intelligence*. De modo a adquirir uma visão mais holística relativamente à temática foram igualmente selecionados participantes de diversas áreas, desde as engenharias, professores e juristas, todos com ligações às áreas do terrorismo ou da IA.

É de salientar que em mais de 50 pedidos de entrevistas apenas foi possível obter a resposta a 27, sendo destes últimos apenas 12 as respostas positivas, o que demonstra um eventual desconhecimento sobre a matéria ou receio em partilha informação (ou porque é residual, ou pela sensibilidade do tema, ou ainda porque subsiste uma resistência em facilitar a comunicação com o mundo académico), o que demonstra a relevância da presente dissertação. De qualquer forma, um dos requisitos do presente trabalho é a qualidade de informação, assim, o objetivo não era a realização de entrevistas em massa, mas sim consultar peritos que possuíssem os conhecimentos necessários e adequados para a participação na presente dissertação.

3.3. *Corpus*

O *corpus* consiste no conjunto de documentos que são submetidos para análise devendo ser respeitadas regras de exaustividade, representatividade, homogeneidade e pertinência (Bardin, 2016). Neste caso, o *corpus* deste estudo abrange um conjunto de 12 entrevistas realizadas a especialistas nas áreas do terrorismo e IA.

3.4. Instrumentos de recolha e análise de dados

Como instrumento para recolha de dados foi escolhida a entrevista. Este é um método que se distingue pela "(…) aplicação dos processos fundamentais de comunicação e de interação humana" (p. 96), facilitando assim a partilha de informação (Marconi & Lakatos, 2017, p. 223). De acordo com Richards (2015) a entrevista permite adquirir ideias e perceções que, à partida, não seriam possíveis de obter de outra forma.

De acordo com os propósitos estabelecidos anteriormente, as entrevistas semiestruturadas revelaram-se como as mais adequadas tendo em conta a importância em obter um discurso aberto e fluído por parte dos entrevistados. Quivy e Campenhoudt (2008) esclarecem que, neste caso, não existe um conjunto rígido de questões que devem ser estritamente seguidas, existe antes um desenrolar flexível e adaptável. No entanto, o guião e a redação das questões são semelhantes para todos os entrevistados (Bryman, 2012). Durante as entrevistas, o investigador deve adquirir sempre uma posição neutra e objetiva (Neuman, 2014).

Desta forma, foi desenvolvido um guião com diversas perguntas abertas (cf. Apêndice D) tendo por base os objetivos e a pergunta de partida já anteriormente mencionados.

Para o presente trabalho, o instrumento de análise de dados do *corpus* selecionado foi a análise de conteúdo que consiste num conjunto de mecanismos de "(…) análise das comunicações visando obter por procedimentos sistemáticos o objetivos de descrição do conteúdo das mensagens indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/receção (variáveis inferidas) dessas mensagens" (Bardin, 2016, p. 48). Esta técnica não incide sobre o próprio funcionamento da linguagem, mas sim nos indicadores do locutor e nos significados e uso social que o mesmo faz na sua comunicação (Quivy & Campenhoudt, 2008).

A realização de uma análise categorial foi o processo de análise escolhido em específico. Esta análise é desenvolvida através do "desmembramento do texto em unidades, em categorias segundo reagrupamentos analógicos" (Bardin, 2016, p. 201).

No que diz respeito ao processo de codificação, as unidades de registo foram selecionadas de acordo com o tema. Para desenvolvimento de estudos comparativos entre grupos e entrevistas semiestruturadas, a codificação temática acaba por ser mais benéfica permitindo identificar visões distintas em diferentes grupos sociais e realizar comparações.

Depois da divisão das várias entrevistas em pequenos excertos foram os mesmos organizados em categorias. Por categoria entende-se um conceito "(…) que abrange elementos ou aspectos com características comuns ou que se relacionam entre si" (Gomes, 2004, p. 70). É de salientar que, dentro da análise de conteúdo, as categorias podem ser definidas a priori ou posteriori (Bardin, 2016). No presente estudo, as mesmas foram elaboradas de uma forma progressiva, sendo constantemente adaptadas após a organização dos vários excertos retirados das entrevistas.

O método de análise de conteúdo pode ser desenvolvido sob uma ótica quantitativa ou qualitativa (Bardin, 2016). Na primeira abordagem o foco está na frequência de aparição de determinados elementos da mensagem recorrendo posteriormente a um método estatístico, sendo mais objetiva, fiel e exata visto a observação ser mais controlada, tornando-se bastante útil para verificar hipóteses por exemplo. Por outro lado, a abordagem qualitativa, a que foi escolhida nesta investigação, recorre a indicadores não suscetíveis de permitir inferências. Este é um processo mais intuitivo, maleável e adaptável. Pode ser utilizada quando o *corpus* é reduzido, estabelecendo-se assim categorias mais descriminantes "por não estar ligada enquanto análise quantitativa a categorias que deem lugar a frequências suficientemente elevadas para que os cálculos se tornem possíveis" (Bardin, 2016, p. 145). No entanto, existem algumas limitações nesta abordagem, nomeadamente a possibilidade de o investigador ser influenciado pelo processo daquilo que o mesmo compreende sobre determinado assunto e existe ainda a falta de objetividade característica nas abordagens quantitativas. Porém, visto o nosso grupo de participantes ser, em certo ponto desigual no que refere às suas profissões, é interessante verificar como, consequentemente, sobre o mesmo assunto, as suas respostas são variadas.

3.5. Procedimento

No âmbito da realização das entrevistas, embora nada substitua o contacto pessoal através de entrevistas físicas, devido à incompatibilidade de horários e motivos profissionais dos entrevistados, algumas foram realizadas através das ferramentas virtuais ZOOM e Skype.

A autorização individual para o tratamento da informação adquirida nas entrevistas foi garantida através da assinatura dos respetivos "Termos de Consentimento Informado" (cf. apêndice C). Com a autorização expressa dos entrevistados, e de modo a facilitar o normal decorrer das entrevistas e partilha das várias ideias, as mesmas foram gravadas com recurso a gravador permitindo a posterior transcrição e análise de dados. Foi garantido aos vários participantes que qualquer informação classificada referente a projetos a serem futuramente desenvolvidos seriam omitidos tal como qualquer elemento que permitisse identificar os entrevistados.

No processo de categorização foram identificados os principais assuntos e posteriormente, as subcategorias com a respetiva codificação, sendo depois associados a estas os segmentos textuais que melhor se ajustavam (cf. apêndice D). A grelha categorial desenvolvida teve por base os objetivos norteados da investigação e principalmente, o conteúdo obtido nas várias entrevistas, sendo assim criadas as seguintes categorias principais:

- A — Categoria **"Existência de IA em Portugal"**. Nesta categoria insere-se todo o conteúdo relacionado com o conhecimento dos nossos participantes sobre a utilização de IA, especificamente em Portugal, no combate ao terrorismo.

- B — Categoria **“Vantagens de IA”.** Nesta categoria insere-se todo o conteúdo relacionado com as possíveis vantagens na utilização de IA para combater o terrorismo.
- C — Categoria **“Dificuldades”.** Nesta categoria insere-se todo o conteúdo relacionado com os desafios na utilização de IA e com os obstáculos na implementação de IA. Sendo estes dois inicialmente duas categorias separadas, devido à possibilidade de vir a colocar em causa o respeito pelo requisito da exclusividade das categorias foram estes dois pontos integrados nesta categoria única.
- D — Categoria **“Necessidade de IA”.** Nesta categoria insere-se todo o conteúdo relacionado com a possibilidade, eficácia e necessidade de se implementar IA em Portugal.

É de salientar que durante o processo de categorização, o cumprimento das regras necessárias para uma correta categorização foi sempre uma prioridade, nomeadamente que fosse explícito e escrito tudo o que poderia ser incluído numa categoria, bem como os seus limites; garantir que cada categoria é exclusiva, ou seja, determinado conteúdo não pode ser passível de ser classificado em uma ou outra categoria; verificar que estas contemplam todos os casos possíveis, cumprimento do requisito da exaustividade, não sendo, no entanto, as categorias demasiado amplas de acordo com o requisito da homogeneidade. Por fim, exige-se que as categorias sejam objetivas, sem subjetivismos, ou seja, os mesmos dados, aos olhos de outro investigador, devem ter uma classificação igual (Bardin, 2016).

Capítulo IV. Apresentação e Discussão dos Resultados

4.1. Existência de inteligência artificial em Portugal

De modo a adquirir contributos para responder à pergunta de partida inicialmente estabelecida, os entrevistados foram questionados sobre a existência de IA para o combate ao terrorismo em Portugal

Rapidamente foi possível verificar que a grande maioria dos participantes não tinha a certeza ou desconhecia (A.3) totalmente a existência do uso destes instrumentos, não só para o combate ao terrorismo como para outros crimes. Porém, existia bastante conhecimento relativamente a outras polícias europeias, como se constata nas respostas abaixo:

Não tenho ideia que exista. (E9)

Eu pessoalmente não, não tenho qualquer conhecimento. (E5)

Relativamente a outras Forças ou Serviços de Segurança nacionais também não tenho conhecimento da existência de IA. (E7)

Não tenho conhecimento da existência destas em Portugal, não quer dizer que não haja. (E4)

Existem ferramentas com base em inteligência artificial que são utilizadas por várias policias europeias e por várias forças de segurança europeias, inclusive participamos num projeto de investigação (…) e nesse projeto explorámos várias vertentes do tratamento de dados digitais no âmbito da investigação policial, no âmbito da intelligence, e foresight, ou seja na área de prevenção de vários tipos de crime e o terrorismo está obviamente incluído nesse leque de crimes. Aí sim lidamos com algumas ferramentas. Algumas são usadas por várias polícias europeias, não lhe podendo dar detalhes sobre quem utiliza o quê visto que uma boa parte do projeto é de informação classificada – mas existem ferramentas de reconhecimento facial, ferramentas de reconhecimento de matrículas, ferramentas de tradução automática de conteúdo, de identificação de expressões em conteúdo, tanto em texto como conteúdos em áudio. (E3)

Foi ainda claro que, para alguns participantes, havia uma certa dificuldade em saber ao certo em que área é que, atualmente, a IA poderia existir no combate ao terrorismo, conforma citação infra:

(...) o que poderá ser feito é através do chamado SOCMINT – Social Media Intelligence, talvez aqui podemos perceber que haja alguma inteligência artificial, particularmente com o desenvolvimento de sistemas de algoritmos que permitem a georreferenciação, que permitem a padronização através de narrativa. Eu não sei se isto acontece em Portugal, mas sei que em outros países acontece. (E2)

É de salientar que, em determinados casos, não foi claramente possível perceber se existem ou não sistemas de inteligência artificial em Portugal devido ao cariz classificado que algumas matérias ou projetos em desenvolvimento poderiam ter, atente-se à seguinte resposta:

Por isso, existem algumas ferramentas que podem ser utilizadas, agora que é utilizada especificamente em Portugal, eu desconheço e o que conheço não posso entrar em grandes detalhes sobre os mesmos. (E3)

Embora possa não existir IA em Portugal, vários são os projetos que estão a ser desenvolvidos por várias entidades em conjunto com as Forças e Serviços de Segurança, recorde-se:

Participamos num projeto que se debruça exatamente sobre a deteção e prevenção de ataques contra tecnologia de inteligência artificial utilizadas pelas forças de segurança. (E3)

Após as respostas positivas ou negativas referentes à utilização de IA, rapidamente era acrescentado pelos entrevistados o facto de que Portugal, até ao momento, estar bastante atrasado nesta área. Porém, dois entrevistados mostravam-se com bastante esperança relativamente à mudança deste paradigma, afirmando que a polícia tem caminhado para uma atuação mais preventiva e não tão reativa, podendo isto ser um sinal que esta está mais preparada para a implementação destas tecnologias. Estes últimos entrevistados salientaram que, embora possam não existir ferramentas de IA em Portugal, o nosso país, não se encontra isolado, pertencendo aos quadros de cooperação policial internacional onde são constantemente difundidas várias informações relacionadas com a prática de terrorismo, conforme os seguintes excertos:

Isto é assim, maior parte disto [predictive analyses, antevisão de mass gathering) não é feito com base na fórmula da inteligência artificial, maior parte é feito essencialmente "à unha", através de avatares, de personas que são criadas, que acompanham. Há

sistemas preparados para isso. Tanto quanto sei, está-se um pouco aquém, não sei se entretanto as coisas se alteraram. (E2)

Algumas tecnologias estão a ser implementadas, muitas menos do que aquelas que deveriam estar. (E3)

Em Portugal tem existido um discurso quase esquizofrénico relativamente a este assunto quando mais comentadores negam o evidente: a necessidade das Forças e Serviços de Segurança terem acesso a estas tecnologias. (E7)

Neste momento encontra-se em fase de aprovação o novo Regulamento da EUROPOL que permitirá àquela Agência da U.E. investir na inteligência artificial, cooperar com as multinacionais financeiras e de informação no quadro de investigações que envolvam mais do que um Estado membros, com países terceiros. (E7)

4.2. Vantagens da inteligência artificial no combate ao terrorismo

No que diz respeito às questões relacionadas com as possíveis vantagens do uso de IA no combate ao terrorismo, destacaram-se três categorias, nomeadamente a vigilância, deteção e identificação (B.4), prevenção e deteção *online* (B.2) e análise de grandes quantidades de informações (B.3).

Na subcategoria (B.4) foram agrupados todos os meios e formas de utilização de IA que permitissem a realização de uma vigilância, deteção e identificação de comportamentos perigosos ou suspeitos da prática de um crime. Este agrupamento foi realizado devido ao caráter amplo de determinados termos como por exemplo “videovigilância”. Vários foram os entrevistados que mencionaram o uso de IA para videovigilância como uma das vantagens. No entanto, um sistema de IA de videovigilância pode detetar indivíduos através do som, da imagem, das características faciais, e tal não foi especificado pelos entrevistados. O reconhecimento facial, análise de texto, de imagem e de áudio foram os mais mencionados, tal como os exemplos infra demonstram:

(…) reconhecimento facial. (E2)

(...) análise de imagem, portanto, o reconhecimento facial hoje em dia é quase como os filmes (…) consegue reconhecer caras (…) envelhecer caras (…) disfarçar caras. (…) por exemplo, quando se aplica filtros no Snapchat (…) já não é ficção científica. Consegue imaginar melhor do que eu, o que consegue fazer com isto ao nível do combate ao terrorismo. (E9)

As fotos todas desfocadas e o conseguir aumentar, na altura não era possível, hoje em dia, até com a reconstrução de imagem (...) é possível fazer isso, com alguma margem de erro mas é possível. A parte da imagem está muito evoluída e consegue-se fazer coisas extraordinárias. (E9)

Reconhecimento de objetos perigosos (armas, explosivos) em imagens como muitos objetos – podendo ser úteis, por exemplo, nos pontos de segurança dos aeroportos. (E10)

A deteção de áudio deepfake é essencial ao combate ao terrorismo. (…) Neste contexto, a deteção inteligente é também crescentemente dificultada, merecendo particular atenção. (E12)

No caso particular da PSP, a inteligência artificial pode ser muito importante nos sistemas de videovigilância em espaços públicos, suspeitos da prática de crimes, objetos suspeitos, viaturas furtadas, mas não deve abandonar o HUMINT. (E7)

No que diz respeito à prevenção e deteção *online*, os participantes explicavam como os ciberespaço é o futuro e que, em determinados casos, como na deteção dos *lone wolves*, o patrulhamento de redes sociais parece ser a única solução. Como vantagem nesta temática, houve um grande destaque para a deteção e prevenção de casos de radicalização ou recrutamento *online*, tal como a monitorização de outras plataformas como o *Youtube* ou *Darkweb*, verifique-se as respostas infra:

A radicalização e o extremismo violento podem ser perfeitamente perscrutados em redes sociais, particularmente quando é provinda de lobos solitários ou massive shooter (…) estes têm experiência suficiente para passar underground. As redes sociais são um mundo que nos permite poder ter uma ação preventiva. (E2)

Há comportamentos online nas redes sociais, fóruns de conversação onde é possível detetar alguns padrões que demonstram radicalização (…) seria interessante dispor de ferramentas tecnológicas que identificassem esses padrões. (E8)

Deteção de perfis mais vulneráveis , por exemplo, indivíduos com moderado a elevado potencial de adesão a grupos terroristas ou indivíduos manipuláveis por grupos extremistas. Um exemplo paradigmático destas aplicações é o Moonshot, um método de redireccionamento de vídeos do YouTube para conteúdo positivo e desradicalizar, com base no comportamento de pesquisa online para refutar propaganda (E12)

A atividade na Dark Web deve também ser alvo de um rastreamento atento para potenciar a caracterização de perfis suspeitos e extremistas. (E12)

Vários participantes explicaram como, todos os dias, cada de nós contribui ativamente para o aumento de informação disponível sobre nós próprios e sobre os outros. Que mesmo no âmbito de investigação criminal, é raro o crime que não tem um telemóvel envolvido ou um conjunto de e-mails para ler. Todas essas informações são acumuladas diariamente e, como referido por um entrevistado, não se torna impossível, mas bastante difícil para um humano analisar essa informação sem qualquer auxílio tecnológico. Consequentemente, a análise de grandes quantidades de dados foi sinalizada e um entrevistado demonstrou , através do exemplo de um projeto em execução, como a IA pode ser utilizada neste âmbito, melhorando o trabalho do polícia, como também protegendo o mesmo:

(...) ajuda-nos a olhar para grandes quantidades de informações e, hoje em dia, a informação é o que é mais gerado (…) uma das dificuldades numa investigação é olhar para a quantidade de informação recolhida ou que está disponível, quer esteja disponível publicamente ou recolhida numa ação policial ou apreensão (…) e é humanamente impossível alguém olhar para todas as imagens que estão num disco rígido por exemplo. (E3)

Se nós entendemos aqui a questão da inteligência artificial como tecnologia para analisar informação que está em formato digital, hoje em dia não se consegue fazer praticamente nada sem isso, neste caso, na área do terrorismo é obvio. (E5)

Numa investigação na área de abusos sexuais contra menores (…) a carga psicológica que um agente está exposto ao passar horas e horas ou dias a fio a visualizar este tipo de informação. Em que pode a Inteligência Artificial ajudar aqui? Pode ajudar a selecionar, a filtrar, a direcionar as pesquisas, ou seja, fica mais fácil de "encontrar a agulha no palheiro", ou seja, encontrar aquele pedaço de informação que é relevante para a investigação (…) facilitando o acesso a grandes quantidades de dados sem necessidade que o agente envolvido tenha que visualizar ou escrutinar esses dados manualmente. Imaginando que eu tenho uma base de dados com um milhão de imagens, eu só estou interessado em imagens que têm uma determinada cara. A inteligência artificial permite-nos filtrar todas essas imagens e escolher a que nós queremos. (E3)

Embora tenha sido mencionado poucas vezes, é relevante expor que vantagens como o combate a outro tipo de crimes, principalmente crimes económicos podem igualmente estar associados ao crime de terrorismo. Um entrevistado explicou como é que a IA poderia ser igualmente usada para difundir constantemente informação de contra radicalização, ou seja, dados educacionais que permitissem que pessoas mais vulneráveis não fossem tão facilmente manipuladas pela propaganda extremista que acabam por consumir.

4.3. Dificuldades na utilização e implementação de inteligência artificial no combate ao terrorismo em Portugal

Para perceber quais as dificuldades associadas à IA, foi perguntado aos entrevistados quais seriam, na sua ótica, os desafios existentes referentes à utilização destas ferramentas e quais os obstáculos associados à sua implementação. Independentemente das diferentes carreiras exercidas pelos participantes, estas foram as perguntas com mais participação e material recolhido. De uma forma geral, todas estas dificuldades associadas preocupavam bastante os entrevistados:

> *Sou um bocadinho crítica relativamente a isso, às vantagens que poderíamos ter porque, entre aquela velha balança que se discute sempre nas ciências sociais e também no direito, entre a garantia da segurança e o respeito pelos Direitos, Liberdades e Garantias acho que seria difícil enumerar assim as vantagens sem pensar nos desafios.* (E1)

Num vasto leque de dificuldades, as mais vezes recorrentes estavam ligadas aos direitos, liberdades e garantias; a questões relacionadas com a responsabilidade após um erro do sistema de IA; e a gestão de meios humanos.

Relativamente aos direitos, liberdades e garantias existe uma preocupação geral dos entrevistados quanto ao direito à privacidade e todos os outros direitos associados a este. Como consequências de possíveis erros dos sistemas de IA ou até mesmo da supervisão humana, devido à sua subjetividade, a preocupação de determinadas decisões serem discriminatórias é algo bastante assustador para os entrevistados e bastante difícil de prever. Apenas mencionado por dois entrevistados, devido à utilização constante de vigilância em massa e não apenas de determinados indivíduos de interesse ou suspeitos, surge associada a possibilidade de, repentinamente, o regime democrático português ser alterado:

> *Portugal, há mais de 40 anos felizmente não é um estado autocrático mas nunca sabemos que tipo de regime poderemos vir a ter e estas ferramentas prestam-se muito para a vigilância da população, manipulação e abuso de poder, por isso a sua utilização deve ser regulada de*

alguma forma para garantir que é utilizada para os fins de investigação criminal, do combate ao terrorismo, prevenção do crime em geral, mas não permitir que ela seja usada politicamente ou outros fins ilícitos. (E3)

Para um entrevistado apenas, este medo de violação de determinados direitos é algo sem sentido que apenas contribui para o nosso atraso no combate a este tipo de crime.

Acredito que a relação da inteligência artificial e a violação de direitos individuais seja um falso problema, pois estas questões estão a ser discutidas ao mais alto nível político-diplomático e jurídico europeu e o velho continente talvez seja a região do mundo onde exista uma maior preocupação com esta realidade. (…) Neste sentido, a inteligência artificial e outros aspetos do desenvolvimento tecnológico não serão nem deverão ser incompatíveis com direitos, liberdades e garantias. (E7)

A quem deve ser atribuída a responsabilidade por falha dos sistemas foi igualmente uma preocupação partilhada pela maioria dos participantes, conforma as seguintes respostas:

(…) as taxas de erro ainda são consideráveis, mesmo que 1% é muito pouco, mas 1% pode tramar a vida de algumas pessoas, centenas ou milhares. (E9)

(...) a questão da responsabilidade (…) obtendo um resultado enviesado informado por uma análise errónea, depois de quem é a responsabilidade por conotar determinado indivíduo como suspeito? Será da pessoa que criou o sistema de IA? Quem autorizou a sua implementação na instituição policial? Ou no agente policial que confiou no resultado que o sistema deu? Esta questão preocupa-me muito. (E1)

Associado a esta responsabilidade está a falta de explicação que estes sistemas oferecem, ou seja, um sistema fornece a resposta mas nem sempre é possível perceber o motivo da mesma, abalando a confiança existente na IA, podendo ser estas decisões catastróficas. Correlacionado com esta característica está o modo como a prova pode vir a ser transformada e difícil de obter.

O desafio é este – temos de olhar para a inteligência artificial como uma ferramenta – é essencialmente uma ferramenta e não pode ser mais do que uma ferramenta. Nós não podemos acabar por validar algumas das teorias que a ficção científica desenvolveu (…) de quase se prever o crime, ou seja, de condenar alguém porque conseguimos prever que ela iria cometer um crime (…) Isso faz-se mediante indícios tangíveis. A identificação de padrões e comportamentos online, do meu ponto de vista, nunca poderá constituir um meio

de prova para condenação. A inteligência artificial e outras ferramentas tecnológicas devem sim ser um instrumento de auxílio às forças e serviços de segurança e devem funcionar como sistemas de alerta prévio e não mais do que isso. (E8)

No que diz respeito à gestão dos meios humanos, não todos, mas seis entrevistados mencionam que a falta de pessoas especializadas e com formação qualificada torna o processo de implementação e de utilização bastante difícil. É necessário que existam pessoas para manusear os sistemas, mas também para garantir que existe uma cadeia de produção e de manutenção desenvolvida pelas próprias instituições.

Ainda nesta subcategoria, foi mencionado por um entrevistado as diferenças geracionais presentes numa instituição como a Polícia de Segurança Pública. Existem elementos mais velhos que, comparados com os elementos mais novos, apresentarão imensas dificuldades em lidar com estas novas tecnologias. Porém, este participante explica também que, no caso dos polícias mais novos, não sabe até que ponto os mesmos gostarão de ser substituídos por um *software*. Nesta ótica, um entrevistado apresentou como solução uma reestruturação das carreiras policiais, incluindo uma carreira civil:

Devemos pensar nas carreiras – temos o exemplo da Polícia Judiciária – esta tem a carreira policial, mas também tem uma carreira técnica, promovendo a abertura de concursos de técnicos para engenharia informática, engenharia geoespacial, etc. Na Polícia de Segurança Pública, devemos pensar em reestruturar a carreira técnica, na medida em que precisaremos de peritos na área ciber (engenheiros, técnicos, etc). Defendo que devemos apostar na formação de Oficiais de Polícia, nomeadamente na frequência de cursos técnicos, mestrados e doutoramentos para os especializar na vertente dos sistemas de informação. Em suma, no médio prazo devem ser recrutados recursos humanos, ser reestruturada a carreira técnica e formar Oficiais de Polícia para robustecerem a estrutura tecnológica da PSP. (E7)

Com um grau de importância menor foram apresentadas ainda outras preocupações, nomeadamente o enquadramento legislativo, ou seja, a falta de um regulamento específico para o uso de IA que esclareça todas as dúvidas que vão surgindo ao longo da sua evolução e o facto de o sistema politico legal em Portugal ser pouco flexível não permitindo o acesso a dados, quer para investigação quer para produção de IA.

Com o mesmo grau de importância surgem dificuldades associadas ao investimento, capacidade técnica e possíveis ataques informáticos ou uso indevido da IA. Relativamente ao investimento, os entrevistados mostraram preocupações referentes aos custos diretos e indiretos destes sistemas sendo que apenas 5% do orçamento da PSP acaba por ser para investimento, sendo o restante gasto com pessoal. Relacionado com este desafio surgem as capacidades

técnicas descritas pelos participantes como bastante poucas e as que existem, pouco eficazes, notando também que, visto ser uma área ainda bastante recente, o mesmo é compreensível. Seis participantes afirmam que o uso de IA aumenta a "corrida às armas", mas neste caso, às tecnologias, visto que estes acabam por poder vir também a usar as mesmas para fins ilícitos e indevidos.

Por fim, e por ordem de importância, surge a cultura de segurança, a facilidade de implementação em Portugal e as próprias características dos sistemas de IA. No primeiro, os participantes explicam que, devido à inexistência de ataques de terrorismo em Portugal e sendo este um dos países mais seguros do mundo, estes sistemas não são uma prioridade, por isso não é desenvolvida uma cultura de segurança baseada na prevenção. Com alguma frustração, os participantes explicam que implementar IA em Portugal seria um desafio devido a toda a burocracia associada e que, quando estes sistemas fossem implementados, já seriam obsoletos. Relativamente às características, dois entrevistados referiram que a falta de transparência e de eficácia destes sistemas são desafios pertinentes.

4.4. Necessidade de implementação de inteligência artificial em Portugal

Para explorar a necessidade de implementação de IA no combate ao terrorismo em Portugal foram apresentados vários temas sendo os mesmos enquadrados nas subcategorias de eficácia de IA em Portugal, necessidade de IA em Portugal, risco de ameaça terrorista em Portugal e o processo de implementação em Portugal.

Relativamente ao risco de ameaça terrorista em Portugal, de uma forma geral, os participantes afirmam que a maioria da população considera Portugal um país seguro. Porém, os mesmos explicam que o risco, embora seja inferior ao de países como a Alemanha, França ou Itália, este não é totalmente nulo.

> *O facto de não existir terrorismo é uma face de dois gumes. Por um lado é lisonjeiro e presenteiro que estejamos tão bem colocados em termos securitários nos rankings mundiais.* (E2)

> *As pessoas têm a perceção de que não pode acontecer nada mas obviamente que pode.* (E4)

Ainda referente aos ataques de terrorismo em Portugal, dois participantes mencionaram o ataque terrorista evitado em fevereiro do presente ano na Faculdade de Ciências da Universidade de Lisboa para demonstrar que Portugal não está, de todo, preparado para estas ameaças, nem para reagir nem para prevenir.

Partindo para a temática da necessidade de implementação destas ferramentas, na sua maioria, todos afirmavam que estas ferramentas de IA eram fundamentais, necessárias, urgentes e relevantes:

> *Vivemos naquilo que podemos chamar de paradigma digital (…) as comunicações hoje não são feitas por pombos de correio nem sinais de fumo, são através de mensagens digitais usando aquilo a que chamados de internet ou telemóvel e a quantidade de dados que gera é gigantesca. Considerando que o terrorismo é um desafio global, eu acho que é fundamental usarmos aquilo que chamamos de estado de arte das tecnologias no qual se inclui ferramentas de análise sistemática e com inteligência desses dados. É impossível não o fazer. Possível é, é extremamente ineficiente e ineficaz.* (E5)

No entanto, um entrevistado mostrou-se mais receoso e com precaução.

> *A minha resposta é tendencialmente afirmativa* (E11)

No âmbito da implementação, os participantes afirmam que é uma realidade bastante próxima e inevitável. Durante o processo de implementação, os vários e diferentes contextos de cada país devem ser analisados e tidos em conta. Ainda assim, para um entrevistado, as características de Portugal são fatores positivos no processo de implementação:

> *Sendo um país relativamente seguro, essas ferramentas são provavelmente mais fáceis de implementar porque os comportamentos suspeitos são mais diferentes do que os comuns. Somos um país relativamente homogéneo do ponto de vista sociocultural, não é muito homogéneo, mas mais homogéneo do que países maires comparando com Estados Unidos e França* (E4)

Porém, outro participante explica como a falta de acesso a dados, ou até mesmo a inexistência de ataques de terrorismo pode ser um grande obstáculo nesta implementação.

> *Podemos ter muita dificuldade em fazer modelos porque se não temos dados, ataques, temos um problema. (…) …provavelmente sim [necessário e eficaz?] mas num nicho que faça sentido por exemplo os ciberataques porque esses só têm tendências a aumentar agora em terrorismo tradicional ou político não me parece (…) no entanto devemos relembrar que a Polícia Judiciária pode ter grandes bases de dados relativamente a ataques que conseguiu prevenir.* (E9)

Relativamente à eficácia destas ferramentas para combate ao terrorismo as respostas são, na sua maioria, de dúvida, devido à dificuldade em prever a radicalização *online,* visto que o papel da internet na radicalização é apenas um facilitador e não a causa principal, ou seja, esta prevenção incidiria apenas sobre um grupo bastante reduzido de pessoas. As dificuldades mencionadas no capítulo anterior e a arquitetura do sistema nacional de segurança, mais o facto de os ataques terroristas não diminuírem independentemente das ferramentas de IA existentes em determinados países, tornam de certa forma, estas ferramentas inúteis:

> *Se é eficaz ou não (…) acontece que muitas vezes o terrorismo e sobretudo os indícios de conspiração terrorista acontecem antes de haver indícios de crime, logo não é possível intercetar comunicações se não tenho prova da ocorrência de um crime ou da iminência da ocorrência de um crime. O combate ao terrorismo faz-se muitas vezes antes disto – esse é um problema legal português referente à eficácia da utilização de inteligência artificial. (*E8)

Para que a IA possa ser eficaz é pertinente não abdicar de fontes humanas e do contacto com a população, valorizando constantemente os direitos, liberdades e garantias do cidadão:

> *A aposta na tecnologia não deve implicar um menor investimento na pesquisa junto de fontes humanas. Uma força de segurança de proximidade como a PSP tem um enorme capital de confiança junto dos cidadãos, instituições, universidades, escolas, organizações não governamentais e deverá rentabilizar esse facto, equilibrando o acesso a uma grande diversidade de fontes humanas com a tecnologia, com vista a melhorar a capacidade para identificar potenciais ameaças e riscos*. (E7)

> *Deve ser encontrado um ponto de equilíbrio entre a crença excessiva e obstinada na inteligência artificial, como se de um remédio para todos os males do mundo se tratasse, incluindo o terrorismo, e a proteção absoluta e irrestrita de certos direitos fundamentais desconsiderando o contributo importante que as novas tecnologias podem oferecer para a prevenção e investigação da criminalidade* (E11)

Conclusão

É através do uso de tecnologias que a sociedade muda a um ritmo acelerado, trazendo consigo vários benefícios. No campo da criminalidade as adaptações a esta nova realidade são igualmente visíveis através do uso de ferramentas tecnológicas por organizações terroristas para atingir os seus objetivos de forma mais rápida e eficaz. Tudo aquilo que antes era feito através do contacto físico, exigindo um determinado risco de perigo, passa agora a ser realizado à distância através de um computador ou de um telemóvel, tornando assim o crime de terrorismo muito mais difícil de se prevenir.

É neste contexto de mudança que o presente estudo pretende explorar o papel da tecnologia no combate ao terrorismo, em específico, da inteligência artificial. Entre as várias vantagens esta pode identificar propaganda terrorista *online*, detetar e traduzir conteúdo extremista, identificar novas redes terroristas, analisar grandes quantidades de informação em tempo útil e realizar identificação biométrica. Porém, questões como violação de direitos, liberdades e garantias e uso de IA por grupos terroristas são desafios bastante complexos de resolver. O objetivo da EU, após reconhecer as potencialidades da IA, é ser líder nesta matéria, no entanto, os Estados-Membros salientam não existir um quadro europeu comum referente ao uso de IA.

De forma a entender o atual nível de conhecimento referente à utilização de IA em Portugal no combate ao terrorismo, revelou-se fundamental auscultar peritos na área de terrorismo e de IA através de uma abordagem qualitativa com recurso a entrevistas semi-estruturadas e realizada, posteriormente, uma análise conteúdo, mais especificamente uma análise categorial.

Face à escassez de literatura em Portugal a versar sobre a utilização de IA para o combate ao terrorismo, o presente trabalho de investigação tem como objetivos contribuir para o aumento de conhecimento científico sobre a temática anteriormente mencionada. Foram ainda delineados como objetivos perceber se ferramentas de IA em Portugal serão necessárias e quais as vantagens e desafios na utilização deste tipo de ferramentas para o combate ao terrorismo.

O uso de IA, é um assunto relativamente novo, que por isso, gera dúvidas, incertezas e medos que se verificam também quando analisada a possibilidade de aplicação da IA no combate ao terrorismo.

Respondendo à pergunta de partida, podemos afirmar que, atualmente, o papel da IA em Portugal é ainda muito limitado. Há um grande desconhecimento daquilo que esta ferramenta é na realidade e como se trata de uma área recente, existe receio ou constrangimento de se dizer algo que não seja correto. Embora alguns projetos de IA em desenvolvimento sejam de caráter classificado, a cultura de partilha de informação especializada e a falta de comunicação é notória, registando-se ainda níveis diferentes de conhecimento sobre IA entre os diferentes grupos de entrevistados. Desta forma, sendo uma temática associada à utilização de dados pessoais, torna-se um tema bastante sensível com reduzida discussão, o que conduz a uma falta de estímulo para a produção académica e a falta de orientação e clareza relativamente à proteção de dados.

Por detrás destes pontos poderá estar a pouca capacidade económica de Portugal tal como a sua cultura de segurança, sendo possível concluir que, atualmente, Portugal não parece estar pronto para a implementação de sistemas de IA.

Face a esta nova realidade, o acesso a telemóveis, a computadores e rede móvel, é algo relativamente fácil, permitindo assim a criação e consumo diário de elevadas quantidades de informação. É interessante verificar que, na sua maioria, as vantagens enumeradas foram baseadas nessa mesma realidade. Para novas ameaças, estão a surgir novas ferramentas adaptadas e, para muitos, a IA surge como a única solução para combater o terrorismo. Porém, para o próprio funcionamento destes sistemas de uma forma eficaz, é fundamental manter sempre ligação com uma parte fundamental e estruturada da PSP — a proximidade com o cidadão e a recolha de informação através de fontes abertas.

Sendo os participantes de áreas completamente diferentes, e mesmo naqueles em que os conhecimentos de IA não eram vastos, foi nas perguntas referentes às dificuldades e desafios que foi possível recolher mais material, sendo isto uma demonstração da elevada preocupação existente. No meio dos vários desafios e obstáculos, houve um grande destaque para a proteção dos direitos, liberdades e garantias e para a questão da responsabilidade. De facto, estas questões não são simples nem de rápida resposta, não são «preto ou branco». Quem rapidamente consegue afirmar que a IA é a resposta ideal para o combate ao terrorismo é porque nunca ponderou efetivamente os seus potenciais riscos. Embora os erros humanos possam provocar determinadas consequências, nos instrumentos tecnológicos com autonomia para aprender e tomar decisões, as mesmas podem ser catastróficas, assustadoras e até mesmo provocar danos irreversíveis. Comparando as várias dificuldades, algumas poderão ser de fácil resolução, no entanto, outras serão bastante complexas ou até mesmo impossíveis de resolver como a atual cultura de segurança e o processo de implementação de sistemas de IA em Portugal.

No que diz respeito à implementação de IA em Portugal para combater o terrorismo, a nossa resposta é tendencialmente afirmativa. No entanto, é preciso que esta seja realizada com cautela, progressivamente e aliada a outro tipo de ferramentas não unicamente tecnológicas visto que as decisões de um sistema de IA apenas adquirem valor depois de validadas por um ser humano, por alguém que possuí capacidades de bom senso, capacidades que permitem uma análise mais profunda e de análise de contexto. É de salientar que estes elementos responsáveis por esta validação devem ser pessoas formadas para tal, estando as mesmas sob o dever de sigilo de todas as informações verificadas. Sendo que, em caso de violação destes, é pertinente garantir que existem os mecanismos legais e de reparação de danos prontos para serem utilizados. Acrescentamos ainda que, para a implementação destas ferramentas, o indicador de risco de um ataque terrorista em Portugal não deve ser o único indicador a ter em conta nesta decisão porque é bastante reduzido, mas não é nulo, é apenas inferior comparado com outros países. Não é

prudente, esperar que seja perpetrado um ataque para serem tomadas medidas ao nível político e legislativo. Importa assinalar que, caso alguns sistemas de IA fossem utilizados em Portugal, poderiam não ser tão eficazes devido a eventuais falhas — sistemas bastante arcaicos e obsoletos, falta de meios humanos, pouca formação, enquadramento legislativo e falta de acesso a dados para construir modelos — contribuindo apenas para um desperdício de recursos humanos e financeiros.

Desta forma, consideramos útil destacar algumas recomendações cuja aplicação poderá contribuir para uma implementação gradual de IA em Portugal. Reforçamos que, não estando Portugal uniformemente preparado para esta realidade, o objetivo destas medidas será preparar o país e as FSS para uma maior abertura e interesse para esta nova área que está já presente na nossa sociedade e carecerá de um investimento com a maior brevidade possível, atendendo à velocidade das ameaças e da necessidade de resposta eficiente:

- Criação de um regulamento único semelhante a um manual que abranja todas as matérias relacionadas com inteligência artificial que seja regularmente atualizado;
- Desenvolvimento de mais estudos e debates referentes ao uso de inteligência artificial onde as várias FSS sejam convidadas;
- Reestruturação da carreira policial através da introdução de uma carreira civil atrativa e estimulante de modo a adquirir nos quadros outras áreas como engenharias ou matemáticas;
- Investir na formação policial através da implementação de competências tecnológicas básicas e avançadas, adaptadas às funções.

Cumpridos os objetivos e enunciadas as recomendações, importa evidenciar alguns obstáculos que limitaram, de alguma forma, a realização da presente investigação. O facto de alguns projetos e sistemas de IA serem matéria classificada, bem como a sensibilidade da temática obstaculizou a análise mais aprofundada sobre a existência de ferramentas de IA em Portugal. Acresce a dificuldade na identificação de participantes disponíveis para participar nas entrevistas. Por fim, o facto de o presente trabalho ser de cariz exploratório exigiu um exercício de síntese desafiante em relação a bibliografia diversa sobre o tema da IA que é implementada noutros países para não fazer extrapolações com caso nacional sem a devida precaução.

Por fim, no que diz respeito a investigações futuras, tendo como base este trabalho exploratório, seria interessante analisar o impacto que a IA pode ter na população ou nas FSS, ou até escolher um determinado sistema de IA e aplica-lo à PSP sobre a forma de teste piloto e verificar quais as possíveis vantagens ou desafios.

Referências Bibliográficas

Livros e Capítulos de Livros

Bardin, L. (2016). *Análise de Conteúdo*. Edições 70

Bakunin, M. (1980). *Bakunin on Anarchism*. Sam Dolgoff.

Bryman, A. (2012). *Social Research Methods*. Oxford University Press

Choi, K., Asal, V., Wilkenfeld, J. & Pattipati, K. R. (2013). Forecasting the Use of Violence by Ethno-Political Organizations: Middle Eastern Minorities and the Choice of Violence. In V. S. Subrahmanian (2013). *Handbook of Computational Approaches to Counterterrorism.*

Creswell, J., Poth, C. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE Publications.

Duque, R. (2016). Terrorismo: um olhar sobre a evolução e as particularidades desta forma de violência. In R. Duque, D. Noivo, & T. A. Silva (Eds.), *Segurança Contemporânea* (1th ed., pp. 131-147). PACTOR.

Elias, L., & Guedes, A. (2010). *Controlos Remotos: dimensões externas da segurança interna em Portugal*. Almedina.

Ekman, P., Rosenberg, E. L. (2005). *What the face reveals: Basic and applied studies of spontaneous expression using the facial action coding system* (2.ª ed.). Oxford University Press.

Gomes, R. (2004). *A análise de dados em pesquisa qualitativa*. Vozes.

Hoffman, B. (2006). *Inside Terrorism.* Columbia University Press.

Horgan, J., & Braddock, K. (2012). Introduction from the Editor. In J. Horgan, & K. Braddock (Eds.), *Terrorism Studies: A Reader* (ed., pp. 8). Routledge.

Martins, R. F. C. (2010). Acerca de “terrorismo” e de “terrorismos”. EUROPRESS.

Marconi, M., Lakatos, E. (2017). *Fundamentos de Metodologia Científica*. Atlas.

Moreira, A. (2004). *Insegurança sem Fronteiras*: o Martírio dos Inocentes. Almedina.

Neiva, L. (2020). *Big Data na investigação criminal - desafios e expectativas na união europeia*. Edições Húmus, Lda. e Autora.

Neuman, W. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Pearson.

Oliveira, A. (2019*). Inteligência Artificial*. Fundação Francisco Manuel dos Santos

O’Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin.

Pennebaker, J. W., & Chung, C. K. (2008). Computerized Text Analysis of Al-Qaeda Transcripts. In K. Krippendorff & M. A. Bock (Eds.), *The Content Analysis Reader* (pp. 453–465). Sage.

Quivy, R., & Campenhoudt, L. (2008). *Manual de Investigação em Ciências Sociais.* Gradiva.

Richards, L. (2015). *Handling Qualitative Data: A Practical Guide*. SAGE Publications.

Russel, J. S., & Norvig, P. (2010). *Artificial Intelligence - A Modern Approach*. Prentice Hall

Sageman, M. (2008). *Leaderless jihad: terror networks in the twenty-first century*. University of Pennsylvania Press.

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses* (1.ª ed.). Universidade Lusíada Editora.

Schmid, A. P., & Jongman, A. J. (1988). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. Transaction Publishers.

Simões, M. J. (2004). Terrorismo(s) e Uso das Tecnologias da Informação e da Comunicação. In A, Moreira (Eds.), *Terrorismo* (2th ed., pp. 508). Almedina.

Subrahmanian, V. S. (2013). *Handbook of Computational Approaches to Counterterrorism*. Springer.

Artigos de revistas científicas

Adamopoulou, E., Moussiades, L. (2020). An Overview of Chatbot Technology. *Artificial Intelligence Applications and Innovations*.

Alaerts, K, Nackaerts, E., Meyns, P., Swinnen, P. S., Wenderoth, N. (2011). Action and Emotion Recognition from Point Light Displays: An Investigation of Gender Differences. *PLOS One*, 6(6). http://doi%2F10.1371%2Fjournal. pone.0020989.

Alpers, G. W., Winzelberg, A. J., Classen, C. (2005). Evaluation of Computerized Text Analysis in an Internet Breast Cancer Support Group. *Computers in Human Behavior*, 21(2), pp. 361–376. https://doi.org/10.1016/j.chb.2004.02.008.

Andrei, V., Cucu, H., Burileanu, C. (2019). Overlapped speech detection and competing speaker counting—Humans versus deep learning. *IEEE Journal of Selected Topics in Signal Processing*, 13(4), 850–862. https://10.1109/JSTSP.2019.2910759.

Araújo, E. (2008).Technology, gender and time: A contribution to the debate. *Gender, Work & Organization,* 15(5), 477-503. https://doi:10.1111/j.1468-0432.2008.00414.x.

Bakker, E. & Van Zuijdewijn, J. (2015). *Lone-Actor Terrorism: Definitional Workshop.* Countering Lone-Actor Terrorism Series No. 2.

Boof, S., Ferreira, N. (2016). Análise dos benefícios sociais da bitcoin como moeda. *Anuario Mexicano de Derecho Internacional*, 16, 499-523. https://doi.org/10.22201/iij.24487872e.2016.16.534

Boulamwini, J., Gebru, T. (2018).Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81,1–15

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, 82(5), 977-1008. https://doi.org/10.1177/0003122417725865.

Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Martenson, C., & Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics*, 2(1), 11.

Chan, J., & Moses, L. (2015). Is Big Data challenging criminology? *Theoretical Criminology*, 20(1), 21-39. https://doi.org/10.1177/1362480615586614.

Choo, K., Smith, R., & McCusker, R. (2007). *The Future of Technology-Enabled Crime in Australia. Trends & Issues in Crime & Criminal Justice*, *341*.

Chung, K.,Pennebaker, W. (2011). Using Computerized Text Analysis to Assess Threatening Communications and Actual Behavior. *National Academic Press*, pp. 3–32.

Cook J., Vale, G. (2019). From Daesh to 'Diaspora' II: The Challenges Posed by Women and Minors After the Fall of the Caliphate. *International Centre for the Study of Radicalisation*, 12(6).

Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting Linguistic Markers for Radical Violence in Social Media. *Terrorism and Political Violence*, 26(1), 246–256. https://doi.org/10.1080/09546553.2014.849948.

Conway, M. (2006). Terrorist use of the Internet and Fighting Back. *Information and Security: An International Journal*, 19, p. 17. http://dx.doi.org/10.11610/isij.1901.

Costa, D. (2004). Sociedade de controle. *São Paulo em perspectiva, 18*(1), 161-167. https://doi.org/10.1590/S0102-88392004000100019.

Crenshaw, M. (1992). Current research on terrorism: the academic perspective. *Studies in Conflit & Terrorism*, 15 (1), 1-11. https://doi.org/10.1080/10576109208435887.

Custers, B. (2012). Technology in Policing: Experiences, Obstacles and Police Needs. *Computer Law & Security Review,* 28(1), 62–68. https://doi.org/10.1016/j.clsr.2011.11.009.

Davis, R. B. (2006). Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance. *CommLaw Conspectus*, 15(119), 119-186.

Drewer, D., Miladinova, V. (2017). The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation. *Computer Law & Security Review*, *33*(3), 298-308. https://10.1016/j.clsr.2017.03.006.

Ekman, P. (1970). Universal Facial Expressions of Emotion. *California Mental Health Research Digest*, 8(4), pp. 151–158.

Ernst, S., & Kop, N. (2018). Zicht op Technologische Ontwikkelingen Binnen de Politie. *Cahiers Politiestudies*, *48*, 227–244.

Ferreira, S. (2014). A sociedade da informação como sociedade de disciplina, vigilância e controle. *Información, cultura y sociedad*, (31), 109-120.

Fernandes, F. (2020). Inteligência Artificial. Desafios e Oportunidades para a Polícia. *Polícia Portuguesa*, 5(2), pp. 30-35.

Fessler, D. M. T., Holbrook, C., Snyder, J. K. (2012). Weapons Make the Man (Larger): Formidability Is Represented as Size and Strength in Humans. *PLOS ONE*, 7(4) https://doi:/10.1371/journal.pone.0032751.

Ganor, B. (2002). Defining terrorism: is one man's terrorist another man´s freedom fighter?. *Police Practice and Research*, 3 (4), 287–304. https://doi.org/10.1080/1561426022000032060.

Ganor, B. (2021). Artificial or Human: A New Era of Counterterrorism Intelligence?. *Studies in Conflict & Terrorism, (44)*7, 605-624. https://doi.org/10.1080/1057610X.2019.1568815.

Gill, P., Horgan, J., & Deckert, P. (2014). Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. *Journal of Forensic Sciences*, 59(2), 425–435. https://doi.org/10.1111/1556-4029.12312.

Goodfellow, I., Papernot, N., Huang, S., Duan, R., Abbeel, P., & Clark, J. (2017, Fevereiro 24). Attacking Machine Learning with Adversarial Examples. *Open AI*. https://openai.com/blog/adversarial-example-research/.

Gonçalves, M. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. *Information & Communications Technology Law*, 26(2), 90-115. https://doi.org/10.1080/13600834.2017.1295838.

Hardt, M., Price, E., & Srebro, N. (2016). Equality of Opportunity in Supervised Learning. *Computer Science, Mathematics*. https://www.semanticscholar.org/paper/Equality-of-Opportunity-in-Supervised-Learning-Hardt-Price/d42b11ce90c9c69a20ed015b73dc33e0e4100a7b.

Hecker, M. (2018). 137 Shades of Terrorism: French Jihadists Before the Courts. *Security Studies Center*, 29, 9-41.

Hert, P., & Lammerant H. (2017). Predictive Profiling and its Legal Limits. Effectiveness gone forever. *Amsterdam University Press*, 29(32), 145-173.

Hosseini, H., Xiao, B. and Poovendran, R. (2017). Google's Cloud Vision API Is Not Robust To Noise. *Cornell Research Repository*. https://arxiv.org/pdf/1704.05051.pdf.

Jackson, R. (2007). An analysis of EU counterterrorism discourse post-September 11. *Cambridge Review of International Affairs*, 20 (2), 233-247. https://doi.org/10.1080/09557570701414617.

Jessee, D. D. (2006). Tactical Means, Strategic Ends: Al-Qaeda Use of Denial and Deception. *Terrorism and Political Violence*, 18 (3) p. 379. https://doi.org/10.1080/09546550600751941.

Kissinger, H. (2018, Junho). How the Enlightenment Ends. *The Atlantic*. https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-humanhistory/559124/.

Krahmann, E. (2007). Private Military and Security Companies, Territoriality and the Transformation of Western Security Governance. *The Diffusion of Power in Global Governance*, 38-70.

Kubler, K. (2017). State of urgency: Surveillance, power, and algorithms in France's state of emergency. *Big Data & Society*, 4(2), 1-10. https://doi.org/10.1177/2053951717736338.

Larson, J., Mattu, S., Kirchner, L., Angwin, J. (2016, Maio 23). *How We Analyzed the COMPAS Recidivism Algorithm*. ProPublica. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

Levine, E. S., Tisch, J., Tasso, A. & Joy, M. (2017). The New York City Police Department's Domain Awareness System. *Interfaces*, 47(1), 70–84. https://doi.org/10.1287/inte.2016.0860.

Madakam, S., Ramaswamy R., Tripathi, S. (2005). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 3(5), p. 165. https://doi: 10.4236/jcc.2015.35021.

Mahesh, B. (2019). Machine Learning Algorithms – A review. *International Journal of Science and Research,* 9(1), 381. https://10.21275/ART20203995.

Meloy, J.R., Hempel, A. G., Mohandie, K., Shiva, A. A., & Gray, B. T. (2001). Offender and offense characteristics of a nonrandom sample of adolescent mass murderers. *Journal of the American Academy of Child & Adolescent Psychiatry,* 40(6), 719–728.

Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology: warning behaviors in threat assessment. *Behavioral Sciences & the Law*, 30(3), 256–279. https://doi.org/10.1002/bsl.999.

Mullen, P. E., James, D. V., Meloy, J. R., Pathé, M. T., Farnham, F. R., Preston, L., Berman, J. (2009). The fixated and the pursuit of public figures. *Journal of Forensic Psychiatry & Psychology,* 20(1), 33–47. https://doi.org/10.1080/14789940802197074.

Munk, T. B. (2017). 100,000 false positives for every real terrorist: Why anti-terror algorithms don't work. *First Monday*, 22(9). https://doi.org/10.5210/fm.v22i9.7126.

Nomikos J., & Liaropoulos, A. (2010) Truly Reforming or Just Responding to Failures? Lessons Learned from the Modernisation of the Greek National Intelligence Service. *Journal of Policing, Intelligence and Counter Terrorism, 5*(1), 28-41. https://doi.org/10.1080/18335300.2010.9686939.

Newman, M. L., Groom, J. C., Handelman, D. L. (2008). Gender Differences in Language Use: An Analysis of 14,000 Text Samples. *Discourse Processes*, 45(3), pp. 211-236. https://doi.org/10.1080/01638530802073712.

Pennebaker, J. W., Mayne, T. J. (1997). Linguistic Predictors of Adaptive Bereavement. *Journal of Personality and Social Psychology*, 72(4), pp. 863-871. https://doi.org/10.1037/0022-3514.72.4.863.

Pennebaker, J. W., Stone, D. L. (2003). Words of Wisdom: Language Use Over the Lifespan. *Journal of Personality and Social Psychology*, 85(2), pp. 291-301. http://doi:10.1037/0022-3514.85.2.291.

Pugliese, J. (2008). Biotypologies of Terrorism. *Cultural Studies Review*, 14(2), pp. 49–66. https://doi.org/10.5130/csr.v14i2.2071.

Rademacher, T., Wischmeyer, T. (2020). *Regulating Artificial Intelligence*. 225-254. https://doi.org/10.1007/978-3-030-32361-5_10.

Ramakrishnan, N., Butler, P., Muthiah, S., Self, N., Khandpur, R., Saraf, P., Wang, W., Cadena, J. Vullikanti, A., Korkmaz, G., Kuhlman, C., Marathe, A., Zhao, L., Hua, T., Chen, F., Lu, C., Huang, B., Srinivasan, A., Trinh, K., Getoor, L., Katz, G., Doyle, A., Ackermann, C., Zavorin, L., Ford, J., Summers, K., Youssef, F., Arredondo, J., Gupta, D., Mares, D. (2014). Beating the News with EMBERS: Forecasting Civil Unrest using Open Source Indicators. *Computer Science, Mathematics*. 10.1145/2623330.2623373.

Rhodes, K. A. (2002). *National Preparedness: Technologies to Secure Federal Buildings*. United States General Accounting Office, pp. 12 -14.

Shawar, A., Atwell, B. A. (2007). Chatbots: are they really useful? *Journal for Language Technology and Computational Linguistics*, 22 (1), pp. 29 – 49.

Spaaij, R. (2015). Lone Actors: Challenges and Opportunities for Countering Violent Extremism. In A. Richman, & Y. Sharan. (Eds.), *Lone Actors – An Emerging Security Threat* (pp. 120-131). IOS Press.

Thomas, T. L. (2003). Al-Qaeda and the Internet: the Danger of Cyberplanning. *Parameters*, (33)1, pp. 115-116. https://doi:10.55540/0031-1723.2139.

Tibbetts, P. S. (2002). Terrorist Use of the Internet and Related Technologies. *School of Advanced Military Studies*, pp. 12-15.

Tolan, S., Miron, M., Gomez, E., Castillo, C., (2019). Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia. *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law*, 83-92. https://doi.org/10.1145/3322640.3326705.

Townsend, J. (2014). Online chilling effects in England and Wales. *Internet Policy Review*, *3*(2). https://doi.org/10.14763/2014.2.252.

Turing, A. M. (1950). Computing machinery and intelligence. *Mind,* 59 (236), 433—460. https://doi.org/10.1093/mind/LIX.236.433.

Van der Vlist, F. N. (2017). Counter-Mapping Surveillance. A Critical Cartography of Mass Surveillance Technology After Snowden *Surveillance & Society*, 15(1), 137-157. https://doi.org/10.24908/ss.v15i1.5307.

Wagner, A. (2005). Terrorism and the Internet: Use and Abuse. *Fighting Terror in Cyberspace*, 1-28. https://doi/10.1142/9789812703255_0001.

Wagner, A. (2007). Intelligence for Counter-Terrorism: Technology and Methods. *Journal of Policing, Intelligence and Counter Terrorism, 2*(2), 48-61. https://doi.org/10.1080/18335300.2007.9686897.

Weimann, G. (2005). How Modern Terrorism Uses the Internet. *The Journal of International Security Affairs,* 8.

Wulf, H. (2007). Challenging the Weberian Concept of the State: The Future of the Monopoly of Violence. *The Australian Centre for Peace and Conflict Studies, 9*(1), 4-29.

Publicações institucionais

Azani, E., Koblenz-Stenzler, L., Atiyas-Lvovsky, L. (2020). The Far Right Ideology, Modus Operandi and Development Trends. *International Institute for Counter-Terrorism*.

Behr, V. I., Reding, A., Edwards, C., Gribbon, L. (2013). Radicalisation in the Digital Era: The use of the Internet in 15 Cases of Terrorism and Extremism. *RAND Europe*. http://doi: 10.1214/07-EJS057.

Davis, P. K., Cragin, K. (2009). *Social Science for Counterterrorism: Putting the Pieces Together*. RAND Corporation.

Dechesne, F., Dignum. V., Bierger, J., & Zardiashvili, L. (2019). Long-term Research Strategy for Artificial Intelligence and Ethics at the Police. Dutch National Police. https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/artificiele-intelligentie-en-ethiek-bij-de-politie/research-strategy-ai-ethics-dutch-police-final.pdf.

Ellis, C., Pantucci, R., Zuijdewijn, J. de R. van, Bakker, E., Gomis, B., Palombi, S., & Smith, M. (2016). *Lone-Actor Terrorism Final Report* (Countering Lone-Actor Terrorism Series No. 11). Royal United Services Institute for Defence and Security Studies.

Fundação para a Ciência e Tecnologia. (2021). *AI Portugal 2030. Portuguese National Initiative on digital skills*. https://www.sgeconomia.gov.pt/noticias/estrategia-inteligencia-artificial-2030.aspx.

IBM Corporation. (2017). *IBM i2 Analyst's Notebook Discover and deliver actionable intelligence*. Industry Solutions. Retrieved from https://www.ibm.com/downloads/cas/QNGO6RNA.

Ionescu, B., Ghenescu, M., Rãstoceanu, F., Roman, R., Buric, M. (2020). Artificial Intelligence Fights Crime and Terrorism at a New Level. *IEEE Computer Society.*

Jensen, M., James, P., LaFree, G., Lichtenstein, A., Yates, E. (2018). The Use of Social Media by United States Extremists. *National Consortium for the Study of Terrorism and Responses to Terrorism.*

Koper, C. S., Lum, C., Woods, D. J., & Hibdon, J. (2015). *Realizing the Potential of Technology in Policing. A Multisite Study of the Social, Organizational and Behavioural Aspects of Implementing Policing Technologies.* National Institute of Justice. http://cebcp.org/wp-content/evidence-based-policing/ ImpactTechnologyFinalReport.

Liv, N. (n.d). Crime Prediction Technologies. *International Institute for Counter-Terrorism*.

McKendrick, K. (2019). *Artificial Intelligence Prediction and Counterterrorism*. International Security Department. https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf.

McKinsey Global Institute (2017). *10 imperatives for Europe in the age of AI and automation*. McKinsey & Company. https://www.mckinsey.com/featured-insights/europe/ten-imperatives-for-europe-in-the-age-of-ai-and-automation.

North Atlantic Treaty Organization (2006). Riga Summit Declaration - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006. *NATO Press Releases.* http://www.nato.int/docu/pr/2006/p06-150e.htm.

Weimann, G. (2018). Going Darker? The Challenge of Dark Net Terrorism. *Wilson Center*.

Weiman, G., Masri, N. (2020). Virtual Hate: Far Right Terrorism in Cyberspace. *International Institute for Counter Terrorism*.

Woodward, J. D. (2001). Biometrics: Facing Up to Terrorism. *RAND Corporation*, 4.

World Economic Forum. (2022). *The Global Risks Report 2022*. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Fontes eletrónicas

Cagle, M. (2016, Outubro 11). *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color.* ACLU Northern California. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

DLive (s.d). *Welcome to DLive*. https://community.dlive.tv/about/welcome-letter/.

IBM (2020). *What is natural language processing?* https://www.ibm.com/cloud/learn/natural-language-processing.

Instagram (s.d). *O que é o Instagram?* https://help.instagram.com/424737657584573.

Lo, C. (2015, Novembro 8). *Safer with data: protecting Pakistan's schools with predictive analytics*. Army Technology. http://www.army-technology.com/features/featuresafer-with-data-protecting-pakistans-schools-with-predictive-analytics-4713601/.

Sageman, M. (2008, Outubro 8). *The Next Generation of Terror.* Foreign Policy. https://foreignpolicy.com/2009/10/08/the-next-generation-of-terror/.

Sovrnmarketing (2010, Maio 10). *Website Crawling: A Guide on Everything You Need to Know.* SOVRN. https://www.sovrn.com/blog/website-crawling-information/

Steam (s.d). *Sobre*. https://store.steampowered.com/about/.

Telegram (s.d). *What is Telegram?.* https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here

Twitch (s.d). *Sobre*. https://www.twitch.tv/p/pt-pt/about/.

USGS (s.d). *What is remote sensing and what is it used for?.* https://www.usgs.gov/faqs/what-remote-sensing-and-what-it-used.

Youtube. (s.d). *Alguma vez se questionou como funciona o YouTube?.* https://www.youtube.com/howyoutubeworks/.

Documentação da União Europeia

Agência da União Europeia para os Direitos Fundamentais. (2020). *Getting the future right – Artificial intelligence and fundamental rights*. Retrieved from https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights.

Comissão Europeia. (2018). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Plano Coordenado para a Inteligência Artificial*. COM (2018) 795 final. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52018DC0795.

Comissão Europeia. (2019). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Aumentar a confiança numa inteligência artificial centrada no ser humano.* COM (2019) 168 final. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52019DC0168.

Comissão Europeia. (2020a). *Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*. COM(2020) 65 final. Retrieved from https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf.

Comissão Europeia (2020b). *Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da ia, da internet das coisas e da robótica comissão europeia*. COM(2020) 64 final. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020DC0064.

Comissão Europeia. (2021). *Regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial)*

e altera determinados atos legislativos da união. COM (2021) 206 final. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206.

Comissão dos Assuntos Jurídicos. (2021). *Relatório sobre a inteligência artificial: questões de interpretação e de aplicação do direito internacional na medida em que a UE é afetada nos domínios da utilização civil e militar e da autoridade do estado fora do âmbito da justiça penal.* Retrieved from https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_PT.html.

Committee of experts on terrorism (2008). *Profiles on Counter-Terrorist capacity*. Conselho da Europa. https://rm.coe.int/1680641014.

Conselho da União Europeia. (24 de novembro de 2005). *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*. 14781/1/05. Retrieved from https://data.consilium.europa.eu/doc/document/ST-14781-2005-REV-1/en/pdf.

Decisão Quadro do Conselho, de 13 de junho. *Conselho da União Europeia* n.º 2002/584/JAI.

Europol. (2017). European Union Terrorism Situation and Trend Report 2017. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/tesat2017_0.pdf.

Europol. (2018). *European Union Terrorism Situation and Trend Report 2018*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european- union-terrorism-situation-and-trend-report-2018-tesat-2018.

Europol. (2019). *European Union Terrorism Situation and Trend Report 2019*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/terrorism- situation-and-trend-report-2019-te-sat.

Europol. (2020). *European Union Terrorism Situation and Trend Report 2020*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european- union-terrorism-situation-and-trend-report-te-sat-2020.

Europol. (2021). *European Union Terrorism Situation and Trend Report 2021*. Retrieved from https://www.europol.europa.eu/publications-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-tesat#downloads.

Office for the Coordination of Humanitarian Affairs. (2021). *Peer review framework for predictive analytics in humanitarian response*. Centre for Humanitarian Data. https://reliefweb.int/report/world/peer-review-framework-predictive-analytics-humanitarian-response-march-2020.

Organização das Nações Unidas (2004). Resolução 1566, Conselho de Segurança das Nações Unidas, S/RES/1566, p.2.

Parlamento Europeu (2020). *Proposta de resolução do Parlamento Europeu sobre a inteligência artificial: questões de interpretação e de aplicação do direito internacional na medida em que a UE é afetada nos domínios da utilização civil e militar e da autoridade do Estado fora*

do âmbito da justiça penal. Retrieved from https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_PT.html#top.

Parlamento Europeu e Conselho Europeu (2006). *Diretiva 2006/42/CE relativa às máquinas e que altera a Diretiva 95/16/CE (reformulação).* Retrieved from https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:32006L0042.

Parlamento Europeu e Conselho Europeu (2016). *Diretiva (UE) 2016/680 do parlamento europeu e do conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.* Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680.

Parlamento Europeu e o Conselho da União Europeia (2016). *Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE* (Regulamento Geral sobre a Proteção de Dados). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

OCHA (2021). *Peer review framework for predictive analytics in humanitarian response*. Centre for Humanitarian Data. https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/76e488d9-b69d-41bd-927c-116d633bac7b/download/peer-review-framework-2020.pdf.

Serviço de Estudos do Parlamento Europeu (2019). *A luta contra o Terrorismo*. Parlamento Europeu.

Sistema de Segurança Interna. (2020). *Relatório Anual de Segurança Interna 2019.* Lisboa: Gabinete do Secretário-Geral.

United Nations Interregional Crime and Justice Research Institute (2019). *Artificial intelligence and robotics for law enforcement*. INTERPOL. https://www.europarl.europa.eu/cmsdata/196207/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf.

UNICRI. (2021, Junho 29). *Building knowledge on counter-terrorism in the age of artificial intelligence: threats, opportunities and safeguarding human rights* [Conference presentation abstract]. 2021 Counter-terrorism week. https://www.un.org/securitycouncil/ctc/events/building-knowledge-counter-terrorism-age-artificial-intelligence-threats-opportunities-and.

Legislação Nacional

Decreto-Lei n.º 383/89, Diário da República n.º 255/1989, Série I de 6 de novembro de 1989 - Transpõe para a ordem jurídica interna a Diretiva n.º 85/374/CEE, em matéria de responsabilidade decorrente de produtos defeituosos.

Lei n.º 52/2003, Diário da República n.º 193/2003, Série I-A de 22 de agosto de 2003 - Lei de combate ao terrorismo (em cumprimento da Decisão Quadro n.º 2002/475/JAI, do Conselho, de 13 de Junho) - décima segunda alteração ao Código de Processo Penal e décima quarta alteração ao Código Penal.

Imprensa

ABC News (2007, Novembro 2). *Amman Radisson Targeted in Foiled Millennium Attack.* ABC News. https://abcnews.go.com/WNT/Terrorism/story?id=1296624

Goldman, J. G. (2014, Fevereiro 10). How being watched changes you – without you knowing. *BBC Future*. http://www.bbc.com/future/story/20140209-being-watched-why-thats-good.

Murphy, P. P. (2018, fevereiro 18). *Exclusive: Group chat messages show school shooter obsessed with race, violence and guns*. CNN. https://edition.cnn.com/2018/02/16/us/exclusive-school-shooter-instagram-group/index.html.

Roettgers, J. (2017, Junho 23). *Google Will Keep Reading Your Emails, Just Not for Ads*. Variety. http://variety.com/2017/digital/news/google-gmail-ads-emails-1202477321/.

Dissertações de Mestrado

Chaves, H. A. C. (2017). *A Unidade de Coordenação Antiterrorismo: Contributos para uma Eficiente Coordenação do Contraterrorismo em Portugal* (dissertação de mestrado, não publicada). Retrieved from: https://comum.rcaap.pt/bitstream/10400.26/19934/1/Disserta%c3%a7%c3%a3o%20Final_H%c3%a9lio%20Chaves.pdf.

Liberal, M. O. D. M. (2012). *Terrorismo e tecnologias - a tecnologia numa dupla perspectiva ao serviço e contra o terrorismo* (dissertação de mestrado, não publicada). Retrieved from: https://repositorio.ucp.pt/handle/10400.14/13272.

Oliveira, F. V. M. Q. (2021). *Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação* (dissertação de mestrado, não publicada). Retrieved from: https://run.unl.pt/bitstream/10362/117660/1/TGI0405.pdf.

Rego, P. C. P. (2017). *Terrorismo lone wolf. Uma visão de literatura* (dissertação de mestrado, não publicada). Retrieved from: https://comum.rcaap.pt/bitstream/10400.26/19937/1/2902_Terrorismo_lone_wolf.pdf

Apresentação de conferência

McCarthy, O. (2021, setembro 21). *Artificial Intelligence and the United Nations*. [Apresentação de Conferência]. CERIS FCT Annual Meeting, UNICRI.

Miguéns, M. I. (2016, abril 6). *Aprendizagem, TIC e Redes Digitais*. [Seminário]. Centro Nacional da Educação. Lisboa.

Mitrea, C. A., Mironicã, I., Ionescu, B., Dogaru, R. (2014, setembro 4 – setembro 6). *Multiple instance-based object retrieval in video surveillance: Dataset and Evaluation*. IEEE International Conference on Intelligent Computer Communication and Processing. Romania.

Anexos e Apêndices

Anexos

Anexo 1 – Ataques terroristas na UE de 2015 a 2020

Figura 1. Ataques terroristas na UE, em 2015 - 2018. Fonte: TE-SAT (2019, p. 13)

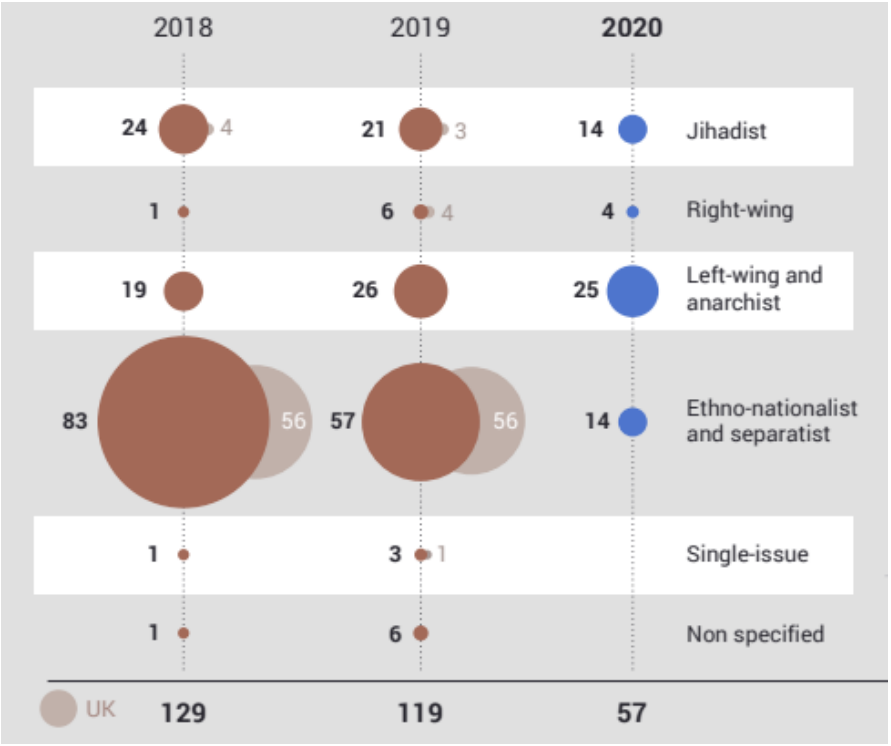

Figura 2. Ataques terroristas na UE, em 2018-2020. Fonte: TE-SAT (2021, p. 14)

Anexo 2 – Mortes e feridos de ataques terroristas de 2016 a 2020

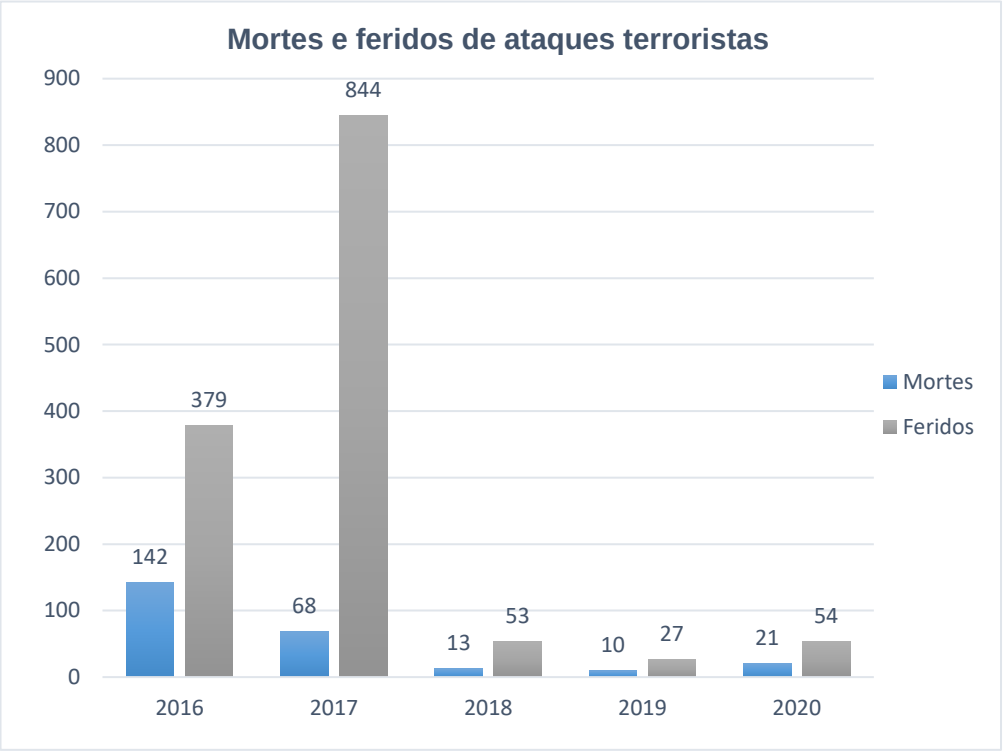

Figura 3. Mortes e feridos de ataques terrorista de 2016 a 2020. Adaptado de TE-SAT (2017, 2018, 2019, 2020, 2021).

Anexo 3 – Propaganda terrorista

Figura 4. Propaganda online de armamento biológico. Fonte: Cyber Report (2018, p. 7)

Figura 5. Aviso online de sites com capacidade de phishing[67]. Fonte: Cyber Report (2018,p. 11)

Figura 6. Folheto sobre um vídeo onde é possível aprender como retirar uma câmara de um telemóvel de modo a que não sejam espiados. Fonte: Cyber Report (2018, p. 15)

Apêndices

Apêndice A – Fases de cada projeto dos países pertencentes à INTERPOL

Tabela 1

Fases de Cada Projeto dos Países Pertencentes à INTERPOL

Fase de desenvolvimento	Exemplo
Fase de conceito	• Algoritmos para identificar veículos suspeitos ou roubados; • Análise de vídeo e de áudio; • *Machine learning* para analisar texto;
Fase de protótipo	• Simulações que permitem apoiar decisões; • Extração de informações para recolher e processar relatórios *online*. • Identificação de comportamentos suspeitos através de dados biométricos; • Identificação de criminosos e pessoas de interesse; • Análise contextualizada de inteligência; • Previsão de protestos políticos e atividades criminosas; • Tradução de áudio; • *Robots* para patrulhar; • Deteção de pornografia infantil;
Fase de avaliação	• Policiamento preditivo para suportar decisões sobre gestão de recursos; • Drones para patrulhar estabelecimentos prisionais e fronteiras; • Análise de vídeo e áudio para monitorizar cidadãos detidos; • Drones para mera vigilância; • Sistemas para detetar, marcar e responder a pessoas ou atividades suspeitas; • *Robots* para comunicar com o cidadão; • Análise de telefonemas;

Aprovado para uso	• Robot de IA para identificar informação legal privilegiada; • Sistema de antecipação de crimes que permite prever temporal e espacialmente um crime de modo a facilitar a gestão de recursos garantindo igualmente a presença policial.

Fonte: UNICRI (2020, p. 19)

Apêndice B – Futuros projetos discutidos na INTERPOL

Tabela 2

Futuros Projetos Discutidos na INTERPOL

Área de estudo	Exemplo
Aplicações robóticas	• *Robots* autónomos para inspecionar objetos suspeitos ou para comunicar com a população através de *chatbots*[s;] • *Robots* que fornecem informações, segurança autónoma e vigilância através de drones; • Mapeamento 3D;
Aplicação de análise de dados	• Automatização de processos de procura; • Deteção de anomalias para identificar transações financeiras suspeitas ou tentativas de lavagem de dinheiro; • Identificação autónoma de burlas *online*; • Automatização de burocracia; • *Profiling*; • Categorização de entidades online tal como compradores e vendedores do mercado negro; • Automatização de deteção e alerta; • Deteção de notícias falsas e uso de internet pelos terroristas; • Ferramentas educacionais baseadas em IA para reabilitar e reintegrar crianças no sistema de justiça; • Prevenir radicalização.
Aplicação de análise preditiva	• Identificação da evolução de fatores de risco e de potencial abuso sexual *online*; • Monitorização de fatores de radicalização numa comunidade específica ou de determinados indivíduos;

	• Prevenção de comportamentos por CCTV através de som, vibrações ou informação não visual;
Aplicações de máquinas de visionamento	• Ferramentas virtuais avançadas de autópsia para ajudar a determinar a causa da morte; • Deteção de comportamento para detetar furtos em flagrante delito; • Deteção facial e ferramentas de validação que permitem identificar criminosos, mesmo a usarem chapéus, máscaras, óculos; • Análise de emoções;

Fonte: UNICRI (2021, pp. 10-12)

[a] Um programa de computador desenvolvido para simular conversas com utilizadores humanos, especialmente através da Internet (Adamopoulou & Moussiades, 2020). Podem ser também chamados de smart bots, agentes interativos ou assistentes digitais. As suas funções englobam entretinimento, negócios, educação e comércio eletrónico (Shawar & Atwell, 2007).

[b] Técnica para processar automaticamente dados pessoais e não pessoais, com o objetivo de desenvolver o conhecimento preditivo a partir dos dados sob a forma de construção de perfis que podem ser subsequentemente aplicados como base para a tomada de decisões. Um perfil é um conjunto de dados correlacionados que representam um indivíduo. A construção de perfis é o processo de descoberta de padrões inesperados entre grande conjuntos de dados (Ferraris et al., 2013, p. 33)

Apêndice C – Termo de Consentimento Informado

Termo de Consentimento Informado

Tomei conhecimento que a estudante finalista do Curso de Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI) da Polícia de Segurança Pública, Aspirante a Oficial de Polícia Inês Patrícia Oliveira Proença, está a desenvolver um estudo sobre a inteligência artificial no combate ao terrorismo, sob orientação da Prof.ª Doutora Raquel Duque.

Neste âmbito foram-me explicados os objetivos do trabalho e foi solicitada a minha colaboração para responder a uma entrevista. Fui informado(a) de que as respostas serão anónimas e que serão gravadas para facilitar a sua análise, sendo destruídos os registos áudio após a sua transcrição. A minha identificação nunca será divulgada e a minha colaboração tem carácter voluntário, podendo desistir em qualquer momento do trabalho. Compreendo que não irá existir qualquer tipo de remuneração ou custos pela minha participação neste estudo. É-me garantido que sempre que necessitar de algum esclarecimento o mesmo ser-me-á facultado.

Fui esclarecido(a) sobre todos os aspetos que considero importantes e as perguntas que coloquei foram respondidas. Fui informado(a) que tenho direito a recusar participar e que a minha recusa não terá consequências para mim.

Aceito, pois, colaborar neste estudo e assino onde indicado.

A investigadora	O(a) entrevistado(a)
_____	_____
Aspirante a Oficial de Polícia	_____
Inês Proença M|157275	

Lisboa, _____ 2022

Apêndice D – Guião de Entrevista

Guião de Entrevista

1 – Existe algum tipo de ferramentas de inteligência artificial no combate ao terrorismo em Portugal?

2 – Se sim, os instrumentos tecnológicos de combate ao terrorismo em Portugal são adequadas, eficientes e eficazes?

3 – Quais poderão ser as vantagens na utilização de inteligência artificial para o combate ao terrorismo?

4 – Quais poderão ser os desafios na utilização de inteligência artificial para o combate ao terrorismo?

5 – Qual o maior obstáculo em Portugal na implementação destas novas ferramentas tecnológicas?

6 – Considera relevante/necessário este tipo de ferramentas para o combate ao terrorismo?

Apêndice E – Quadro Categorial

- **A** – Categoria **"Existência de IA em Portugal"**. Nesta categoria insere-se todo o conteúdo relacionado com o conhecimento dos nossos participantes sobre a utilização de IA, especificamente em Portugal, no combate ao terrorismo.

  A.1 - Subcategoria "**Projetos e Polícias Europeias**". Nesta subcategoria insere-se informação relacionada com projetos em desenvolvimento quer em Portugal quer na Europa por outras polícias.

  Ex.: Existem ferramentas com base em inteligência artificial que são utilizadas por várias policias europeias (…) e participamos num projeto de investigação (…) e nesse projeto explorámos várias vertentes do tratamento de dados digitais (…) (E3).

  A.2 - Subcategoria "**Realidade Tecnológica em Portugal**". Nesta subcategoria insere-se informação relacionada com a relação de Portugal com IA e com a tecnologia no geral.
  Ex.: Ainda há um longo caminho a percorrer, sobretudo quando em comparação com outros estados (…) (E2).

  A.3 - Subcategoria "**Desconhecimento/Não existe**". Nesta subcategoria insere-se informação relacionada com o todo o conhecimento de existência de IA em Portugal para combater o terrorismo.

  Ex.: Não tenho conhecimento daquilo que as nossas forças policias e de segurança utilizam no combate e prevenção do terrorismo. (E3)

- **B** – Categoria **"Vantagens de IA".** Nesta categoria insere-se todo o conteúdo relacionado com as possíveis vantagens na utilização de IA para combater o terrorismo em Portugal.

  B.1 – Subcategoria "**Análise de Grandes Quantidades de Informações**". Nesta subcategoria insere-se informação relacionada com as capacidades de IA de recolha, análise e produção de grandes quantidades de informação.
  Ex.: Na área de levantamento e recolha de informação, a IA parece-me bastante importante. (E2)

  B.2 – Subcategoria "**Prevenção e deteção *online***". Nesta categoria insere-

se informação relacionada com possibilidades de prevenção e deteção *online* de comportamentos associados à radicalização, consumo de propaganda e planeamento de possíveis ataques.

Ex.: A utilização de inteligência artificial poderia ser útil na identificação e sinalização de alguns padrões comportamentais online. (E8)

B.3 – Subcategoria "**Gestão de meios**". Nesta categoria insere-se informação relacionada com as vantagens inerentes à gestão de meios, quer humanos, quer materiais.

Ex.: Maior ganho no tempo (…) e em termos de recursos humanos também se pouparia também. (E1)

B.4 – Subcategoria "**Vigilância e Deteção de Indícios de Perigo**". Nesta categoria insere-se informação relacionada com a vigilância, deteção e identificação de comportamentos perigosos ou suspeitos da prática de um crime. Foi criada esta grande subcategoria devido ao carater amplo de determinados termos como por exemplo "videovigilância". Vários foram os entrevistados que mencionaram o uso de IA para videovigilância como uma das vantagens, no entanto, um sistema de IA de videovigilância pode detetar indivíduos através do som, da imagem, das características faciais, e tal não foi especificado pelos entrevistados.

EX.: No caso particular da PSP, a inteligência artificial pode ser muito importante nos sistemas de videovigilância em espaços públicos (...) (E7)

B.5 - Subcategoria "**Combate a outros crimes**". Nesta categoria insere-se informação relacionada com o uso de IA para o combate a outros crimes que poderão ou não estar associados ao terrorismo.

EX.: (…) a utilização de inteligência artificial para análise de fluxos financeiros suspeitos, deteção de lavagem de dinheiro. (E4)

B.6 - Subcategoria "**Outros**". Nesta categoria insere-se informação relacionada com possíveis vantagens do uso de IA para combater o terrorismo mas que não têm o perfil nem requisitos para serem inseridos em outras subcategorias.

EX.: Promoção de narrativas positivas como forma de corrigir comunicação extremista e violenta (…) (E12)

- C – Categoria **"Dificuldades associadas à IA".** Nesta categoria insere-se todo o conteúdo relacionado com os desafios na utilização de IA e com os obstáculos na implementação de IA. Sendo estes dois inicialmente duas categorias separadas, devido à possibilidade de vir a colocar em causa o respeito pelo requisito da exclusividade das categorias foram estes dois pontos integrados nesta categoria única.

  C.1 – Subcategoria "**Enquadramento Legislativo**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados ao enquadramento legislativo português.
  Ex.: Existe um caminho a percorrer no plano jurídico (E7)

  C.2 – Subcategoria "**Direitos, Liberdades e Garantias**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados a possíveis violações de Direitos, Liberdades e Garantias.

  Ex.: (…) uma dimensão ética (…) e legal que esbarra com a privacidade de dados. Estes são os principais constrangimentos. (E2)

  C.3 – Subcategoria "**Responsabilidade**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados a dúvidas e falta de clareza nos assuntos referentes a responsabilidade em caso de erros e falhas, e consequentemente questões relacionadas com a validade da prova.

  Ex.: Desenvolver processos de regulamentação e certificação para garantir que os sistemas de AI (…) fornecem responsabilidade no caso de uso indevido (E12)

  C.4 – Subcategoria "**Investimento**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados à falta de investimento nas tecnologias em Portugal.

  Ex.: (…) o investimento relativamente reduzido no plano tecnológico, se compararmos com outros países.(E7)

C.5 – Subcategoria "**Capacidade Técnica**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados à capacidade técnica reduzida de Portugal.

Ex.: Não há a tecnologia suficiente. (E2).

C.6 – Subcategoria "**Gestão de meios humanos**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados às gestão de meios humanos, quer a nível motivacional como de existência de efetivo.

Ex.: A resistência à mudança também nunca é muito confessada pelos agentes policiais (…) (E1)

C.7 – Subcategoria "**Ataques informáticos e Uso indevido da IA**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados a possíveis ataques informáticos e uso indevido da IA para fins ilícitos.

Ex.: (…) existem algumas fragilidades que é a própria tecnologia ser sujeita a ataques. (E3)

C.8 – Subcategoria "**Cultura de Segurança**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados à cultura de segurança existente em Portugal.

Ex.: Existe um caminho a percorrer (…) no plano da cultura de segurança. (E7)

C.9 – Subcategoria "**Processo de implementação em Portugal**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos na implementação associados aos processos de implementação em Portugal.

Ex.: Por causa das burocracias e "capelinhas". Se estes dados estão nas minhas mãos eu não vou abrir acesso a mais ninguém (E9)

C.10 – Subcategoria "**Características do Sistema**". Nesta subcategoria insere-se informação relacionada com os desafios na utilização e obstáculos

na implementação associados às próprias características dos sistemas.

Ex.: Persistente falta de transparência e eficácia dúbia da IA (E12)

- D – Categoria **"Necessidade de IA em Portugal".** Nesta categoria insere-se todo o conteúdo relacionado com a as possibilidade, eficácia e necessidade de se implementar IA em Portugal.

  D.1 - Subcategoria "**Eficácia da utilização de IA**". Nesta subcategoria insere-se todo o conteúdo relacionado com a possibilidade de a IA ser um dos métodos mais adequados para combater o terrorismo em Portugal.

  Ex.: Ao nível prático é que não é assim tão eficaz quanto isso (…) (E1)

  D.2 – Subcategoria "**Risco de ameaça em Portugal**". Nesta subcategoria insere-se todo o conteúdo relacionado com a perceção do risco de ameaça de terrorismo em Portugal.
  Ex.: Não digo que o risco em Portugal seja 0, será possivelmente inferior do que na Alemanha ou França ou Itália mas não será 0 (E3)

  D.3 – Subcategoria "**Necessidade de IA**". Nesta subcategoria insere-se todo o conteúdo relacionado com o grau de necessidade de existência de IA em Portugal para combater o terrorismo.

  Ex.: É fundamental investir na Inteligência Artificial. (E7)

  D.4 Subcategoria "**Processo de Implementação de IA**". Nesta subcategoria insere-se todo o conteúdo relacionado com

  Ex.: Podemos ter muita dificuldade em fazer modelos porque se não temos dados, ataques, temos um problema. (…) (E9)

Apêndice F – Codificação

Tabela 3

Codificação

TEMA PRINCIPAL	TEMA SECUNDÁRIO	TEXTO
Existência de IA em Portugal (A)	**Projetos e Polícias Europeias (A.1)**	Lideramos um projeto europeu (…) que está focado não tanto na deteção mas como lidar com os ataques a ferramentas de inteligência artificial e a IOT que são dois novos paradigmas. Existe também o *Computer Security Incident Response Team (CISRT)*, ou seja, uma equipa de resposta a incidentes de segurança. (E3) Participamos num projeto que se debruça exatamente sobre a deteção e prevenção de ataques contra tecnologia de inteligência artificial utilizadas pelas forças de segurança. (E3) Existem ferramentas com base em inteligência artificial que são utilizadas por várias policias europeias e por várias forças de segurança europeias, inclusive participamos num projeto de investigação (…) e nesse projeto explorámos várias vertentes do tratamento de dados digitais no âmbito da investigação policial, no âmbito da *intelligence*, e *foresight*, ou seja na área de prevenção de vários tipos de crime e o terrorismo está obviamente incluído nesse leque de crimes. Aí sim lidamos com algumas ferramentas. Algumas são usadas por várias polícias europeias, não lhe podendo dar detalhes sobre quem utiliza o quê visto que uma boa parte do projeto é de informação classificada – mas existem ferramentas de reconhecimento facial, ferramentas de reconhecimento de matrículas, ferramentas de tradução automática de conteúdo, de identificação de expressões em conteúdo, tanto em texto como conteúdos em áudio. (E3)

	Existem tecnologias que podem ser utilizadas pelas polícias e estas estão atentas a isso, ou seja, há a um nível europeu algum movimento por parte das forças policiais de estarem atentas às ferramentas que surgem. Como resultado deste projeto foi criada uma associação (…) onde o objetivo é utilizar resultados dos projetos de investigação e levar os mesmos a um nível de maturidade no qual possa ser utilizado pelos policias. A associação tem como fundadores (…) e algumas forças policiais (…) e o objetivo é melhorar essas ferramentas e torná-las utilizáveis pelas forças de segurança. (E3)
Realidade Tecnológica em Portugal (A.2)	Isto é assim, maior parte disto [*predictive analyses*, antevisão de *mass gathering*) não é feito com base na fórmula da inteligência artificial, maior parte é feito essencialmente "à unha", através de avatares, de personas que são criadas, que acompanham. Há sistemas preparados para isso. Tanto quanto sei, está-se um pouco aquém, não sei se entretanto as coisas se alteraram. (E2) A colaboração com a sociedade civil e parcerias público privadas nesta área também está muito aquém do que aquilo que poderia ser feito. (E2) Mas tanto quanto sei, desenvolvimento de inteligência artificial ainda está muito precário. (E2) Especificamente para a questão do extremismo violento, tanto quanto sei em termos institucionais a aplicação de tecnologias ainda é extremamente…não muito eficaz e ainda funciona muito aquém daquilo que poderia ser feito. (E2) (…) mesmo em termos de OSINT, eu acho que há muito que poderia ser feito. (E2)

Não se está a apostar na tecnologia suficiente que permita a antevisão de mass gathering (…), de radicalização. (E2)

Ainda há um longo caminho a percorrer, sobretudo quando em comparação com outros estados (…) não só em termos de *software*, de estruturas informáticas, de inteligência artificial. (E2)

Algumas tecnologias estão a ser implementadas, muitas menos do que aquelas que deveriam estar. (E3)

Se hoje em dia a Policia Judiciária utilizar o serviço de correio eletrónico atualizado, o servidor atual já está a utilizar inteligência artificial, portanto hoje em dia os servidores de correio eletrónico já usam estas técnicas. Se houver um Inspetor da Polícia Judiciária ou um Polícia da PSP que use um smartphone para tirar uma fotografia já está a utilizar inteligência artificial porque a probabilidade desse *smartphone* ter algoritmos de inteligência é grande, de certeza que há qualquer coisa. (E5)

Nota-se que a Polícia Judiciária tem feito um grande esforço nos anos, mas eu diria que ainda estamos muito aquém, ainda há muito trabalho a fazer. (E5)

Em Portugal tem existido um discurso quase esquizofrénico relativamente a este assunto quando mais comentadores negam o evidente: a necessidade das Forças e Serviços de Segurança terem acesso a estas tecnologias. (E7)

No entanto, esta tecnologia em Portugal, especialmente no setor público, ainda tem um longo caminho a percorrer. (E7)

Devemos relembrar que Portugal não está isolado do mundo, pois no quadro da cooperação policial internacional são difundidas informações para as Forças e Serviços de Segurança sobre grupos e/ou pessoas radicalizadas, assim como sobre a criminalidade organizada transnacional, verificando-se a monitorização na *darknet* de fóruns e de outros sítios da rede onde é desenvolvida a prática criminal e a difusão de mensagens de ódio e intolerância por parte de grupos terroristas e extremistas. (E7)

Ao nível da União Europeia estas matérias ainda estão a ser discutidas, por exemplo, no âmbito do novo regulamento da EUROPOL, onde irá ser possível a troca de informações com entidades privadas como as grandes multinacionais de informações como o Facebook e Google. (E7)

Neste momento encontra-se em fase de aprovação o novo Regulamento da EUROPOL que permitirá àquela Agência da U.E. investir na inteligência artificial, cooperar com as multinacionais financeiras e de informação no quadro de investigações que envolvam mais do que um Estado membros, com países terceiros. (E7)

Era útil dispor destas ferramentas. (E8)

Na altura fiquei com a ideia que havia gente a trabalhar nessa área. (E9)

Tanto quanto sei, a utilização de ferramentas de inteligência artificial na luta contra o terrorismo e no sistema de justiça penal português é ainda muito incipiente. (E11)

Tem havido um investimento na investigação científica no domínio de IA e criminalidade (…) que poderá levar a uma alteração deste estado de coisas. (E11)

	Paulatinamente temos caminhado para uma lógica preventiva em vez de reativa. (E11)
Desconhecimento/Não existe (A.3)	De que eu tenha conhecimento, não está nenhum software em curso. Do que eu percebi, foi que existiam bastantes projetos em curso, na PSP nem tanto, mas na PJ eles têm bastante reuniões internacionais e há bastantes projetos em desenvolvimento. (E1) A perceção com que fiquei foi que não existe assim nenhum *software* que possam dizer que é de inteligência artificial. (E1) Eu fique com a ideia de que eles [Polícia Judiciária] diziam que não tinham assim nenhum *software*, eles falavam muito do *PredPol*, do *CompStat* e esses de policiamento preditivo, e também do *I2Analyst Notebook*, mas que acabam por não ser de inteligência artificial porque são softwares que não permitem aprender com os dados. (E1) (...) o que poderá ser feito é através do chamado SOCMINT – *Social Media Intelligence*, talvez aqui podemos perceber que haja alguma inteligência artificial, particularmente com o desenvolvimento de sistemas de algoritmos que permitem a georreferenciação, que permitem a padronização através de narrativa. Eu não sei se isto acontece em Portugal, mas sei que em outros países acontece. (E2) Por isso, existem algumas ferramentas que podem ser utilizadas, agora que é utilizada especificamente em Portugal, eu desconheço e o que conheço não posso entrar em grandes detalhes sobre os mesmos. (E3)

Não tenho conhecimento daquilo que as nossas forças policias e de segurança utilizam no combate e prevenção do terrorismo. (E3)

Não tenho conhecimento da existência destas em Portugal, não quer dizer que não haja. (E4)

Eu pessoalmente não, não tenho qualquer conhecimento. (E5)

Não sei. Acredito que existam, e sem entrar em teorias de conspiração, acredito perfeitamente que existam, mas não tenho conhecimento e logo não sei se são utilizadas ou não. (E6)

Ferramenta propriamente dia penso que não. (E7)

Relativamente a outras Forças ou Serviços de Segurança nacionais também não tenho conhecimento da existência de IA. (E7)

Que eu saiba não, não existe. (E8)

Eu estive numa pequena conferência em que havia um artigo em que se fazia a utilização de ferramentas de IA no combate ao terrorismo e lembro-me de que a grande dificuldade era perceber texto em árabe porque as línguas árabes são muito pouco estruturas e as ferramentas que existiam na altura, ainda eram muito pobres e eles tinham uma grande dificuldade em adaptar as ferramentas do inglês para o árabe e isso ficou-me na memória mas não sei mais nada sobre isso, foi a única vez que ouvi mencionar o combate ao terrorismo no que diz respeito a IA. (E9)

Não tenho ideia que exista. (E9)

		Não estou por dentro da tecnologia atualmente utilizada pelas autoridades no combate ao terrorismo. (E10)
Vantagens (B)	**Análise de Grandes Quantidades de Informações (B.1)**	Beneficiaríamos sempre do acesso mais rápido aos dados. (E1) Na área de levantamento e recolha de informação, a IA parece-me bastante importante. (E2) (...) ajuda-nos a olhar para grandes quantidades de informações e, hoje em dia, a informação é o que é mais gerado (…) uma das dificuldades numa investigação é olhar para a quantidade de informação recolhida ou que está disponível, quer esteja disponível publicamente ou recolhida numa ação policial ou apreensão (…) e é humanamente impossível alguém olhar para todas as imagens que estão num disco rígido por exemplo. (E3) Numa investigação na área de abusos sexuais contra menores (…) a carga psicológica que um agente está exposto ao passar horas e horas ou dias a fio a visualizar este tipo de informação. Em que pode a Inteligência Artificial ajudar aqui? Pode ajudar a selecionar, a filtrar, a direcionar as pesquisas, ou seja, fica mais fácil de “encontrar a agulha no palheiro”, ou seja, encontrar aquele pedaço de informação que é relevante para a investigação (…) facilitando o acesso a grandes quantidades de dados sem necessidade que o agente envolvido tenha que visualizar ou escrutinar esses dados manualmente. Imaginando que eu tenho uma base de dados com um milhão de imagens, eu só estou interessado em imagens que têm uma determinada cara. A inteligência artificial permite-nos filtrar todas essas imagens e escolher a que nós queremos. (E3)

A verdade é que, hoje em dia, qualquer crime tem uma componente digital, é raro um crime que não tem um telemóvel envolvido, um e-mail, uma mensagem – o que leva a que a investigação, a recolha e o processamento da prova digital seja uma área fundamental nas forças de segurança. (E3)

Hoje em dia ninguém consegue fazer análise de informação em ambiente digital de forma eficaz e eficiente sem utilizar estado de arte na tecnologia no qual se engloba esta coisa que chamamos de inteligência artificial. (E5)

Se nós entendemos aqui a questão da inteligência artificial como tecnologia para analisar informação que está em formato digital, hoje em dia não se consegue fazer praticamente nada sem isso, neste caso, na área do terrorismo é obvio. (E5)

Muitas, muitas mesmo (…) conseguimos fazer coisas que os seres humanos não conseguem: não só lidar com enormes capacidades de informação, como também detetar padrões que o ser humano não se consegue aperceber. (E6)

No ponto de vista mais técnico, a IA neste momento tem todas as ferramentas para conseguir trabalhar contra o terrorismo, nomeadamente no que diz respeito à análise de dados e ciência de dados. (E9)

(…) capacidade que os sistemas de IA têm de processar grandes quantidades de dados e detetar padrões relevantes nestes. (E10)

Capacidade de generalizar os padrões observados em grandes conjuntos de dados, fornecendo assim uma poderosa ferramenta com a capacidade de prever a ocorrência destes padrões. (E10)

	Identificando padrões de atividade, descobrindo redes de contactos e, em geral, encontrando significado em dados provenientes de múltiplas origens e em quantidades avassaladoras. (E11)
Prevenção e deteção *online* (B.2)	A radicalização e o extremismo violento podem ser perfeitamente perscrutados em redes sociais, particularmente quando é provinda de lobos solitários ou *massive shooter* (…) estes têm experiência suficiente para passar *underground*. As redes sociais são um mundo que nos permite poder ter uma ação preventiva. (E2) Quando falo em *Social Media Intelligence* há várias formas de o fazer – *social network analyses,* através de uma análise do conteúdo utilizando uma *bag of words*. Vamos imaginar, nestes casos da inteligência artificial, vamos pôr – terrorismo, lisboa, terreiro do paço, etc. Varre-se tudo o que é comunicação, outra forma será através de linguagem computacional, portanto há várias fórmulas de poder desenvolver esta *social media intelligence* e há vários *softwares* que o fazem e que não são necessariamente intrusivos e invasivos. (E2) Neste campo em específico do extremismo e radicalismo que pode levar à violência eu acho que a IA aplicadas às comunicações sociais e às redes sociais é um instrumento fundamental. (E2) Temos os [*softwares*] mais básico que permitem análise de rede. Pode ainda ser feito *Social Network Analyses*, no fundo o que vão fazer é um levantamento total dos chamados *Key Actors*, define quem são com base na intensidade de comunicações, define também com o conteúdo de cada comunicação e a partir daí consegue entender mais ao menos uma estrutura em termos organizacionais. (E2)

Há cerca de 6 anos nas redes sociais israelitas e palestinianas, surgiu um apelo aberto nas redes sociais mais especificamente no Facebook e Twiiter, a chamada *intifada* onde foi feito um apelo aos palestinianos para pegarem instrumentos cortantes, e disferir uma facada aleatória num israelita. Isto é um fenómeno interessantíssimo porque houve durante algumas semanas o terror e pânico, houve ataques (…) Neste caso talvez a IA teria verificado isto e evitado. (E2)

As aplicações mais óbvios são aquelas que envolvem analisar tudo o que existe nas redes sociais públicas. (E6)

A utilização de inteligência artificial poderia ser útil na identificação e sinalização de alguns padrões comportamentais *online*. (E8)

Deteção de padrões em textos e outros tipos de comunicação escrita (…) é utilizado tanto no processamento de textos e língua falada como na geração de textos (…) é grande utilidade para monitorizar de forma autónoma comunicações em redes sociais e outros meios escritos. Por exemplo, este tipo de técnicas foi já utilizado para detetar proliferação de discurso extremista em redes sociais ou identificação de *bots* nas redes sociais, responsáveis por geração de desinformação e *fake news* (E10).

Análise de redes sociais (*social network analysis).* (E11)

Deteção de radicalização e subsequente moderação de conteúdos. (E12)

	Modelos avançados de classificação (de conteúdo) ou regressão podem ser desenhado para garantir sensibilidade a variações subtis de linguagem, estilo e conteúdo, bem como para atender a diferentes critérios do que é radicalização. (E12)
	Promoção de narrativas positivas como forma de corrigir comunicação extremista e violenta (…) a IA pode ser usada para selecionar conteúdo polar por forma a promover a reversão de perspectivas extremistas. A apresentação e recomendação de conteúdo positivo em aplicações móveis ou até mesmo na vida real (e.g. bairros sensíveis, formação, comunicação direcionada) é uma direção essencial. (E12)
	Estudos recentes mostram que este tipo de notícias [*fake news*] pode já ser detetada com elevado grau de precisão (>90%) com base no conteúdo de forma isolada e cruzada com outras fontes de informação. (E12)
	Deteção de perfis mais vulneráveis , por exemplo, indivíduos com moderado a elevado potencial de adesão a grupos terroristas ou indivíduos manipuláveis por grupos extremistas. Um exemplo paradigmático destas aplicações é o Moonshot, um método de redireccionamento de vídeos do YouTube para conteúdo positivo e desradicalizador, com base no comportamento de pesquisa online para refutar propaganda. (E12)
	A identificação e monitorização de perfis suspeitos nestas plataformas [plataformas baseados em *crowdfunding*, *mobile banking*, e *blockchain*] recorrendo a avanços da IA é essencial. (E12)
Gestão de meios (B.3)	Maior ganho no tempo (…) e em termos de recursos humanos também se pouparia também. (E1)

	Seria também uma estratégia policial mais eficiente na prática, poupar-se-ia em recursos humanos porque há partida, expectava-se que o software acabasse por substituir aquele trabalho de análise criminal que às vezes tem de ser feito e demora imenso tempo e que exige outros tipos de recursos também. (E1) O sistema ARMOR utiliza técnicas de planeamento (…) para determinar/recomendar a distribuição de patrulhas no aeroporto de Los Angeles por forma a minimizar a possibilidade e o impacto de potenciais ataques (…) Desenvolvido pela mesmo equipa (…) o sistema IRIS utiliza o mesmo tipo de técnica (…) para otimizar o escalonamento e distribuição dos "Federal Air Marshals" pelos voos comerciais americanos (E10).
Vigilância e Deteção de Indícios de Perigo (B.4)	(…) reconhecimento facial. (E2) (…) para analisar redes de comunicação suspeita. (E4) Videovigilância com inteligência artificial a infraestruturas críticas. (E4) (…) para detetar movimentos estranhos, pessoas com comportamentos estranhos. (E4) No caso particular da PSP, a inteligência artificial pode ser muito importante nos sistemas de videovigilância em espaços públicos, suspeitos da prática de crimes, objetos suspeitos, viaturas furtadas, mas não deve abandonar o HUMINT. (E7)

(...) análise de imagem, portanto, o reconhecimento facial hoje em dia é quase como os filmes (…) consegue reconhecer caras (…) envelhecer caras (…) disfarçar caras. (…) por exemplo, quando se aplica filtros no Snapchat (…) já não é ficção científica. Consegue imaginar melhor do que eu, o que consegue fazer com isto ao nível do combate ao terrorismo. (E9)

As fotos todas desfocadas e o conseguir aumentar, na altura não era possível, hoje em dia, até com a reconstrução de imagem (...) é possível fazer isso, com alguma margem de erro mas é possível. A parte da imagem está muito evoluída e consegue-se fazer coisas extraordinárias. (E9)

(…) análise de texto. (E9)

Reconhecimento facial, que pode ser realizado de forma autónoma ou através de técnicas de IA que permitem aumentar artificialmente a resolução de imagens ou vídeos, facilitando assim a sua visualização por utilizadores humanos. (E10)

Reconhecimento de objetos perigosos (armas, explosivos) em imagens como muitos objetos – podendo ser úteis, por exemplo, nos pontos de segurança dos aeroportos. (E10)

Avaliação de risco de passageiros de transportes coletivos, identificação de pessoas através de CCTV, deteção de comportamentos violentos, etc. (E11)

O recurso a GANs (*Generative Adversarial Networks*), em particular a MorGAN (*Morphing through Generative Adversarial Networks*), tem sido usado para falsificação de documentação de viagem ou passaportes de vacinas. A exploração das mesmas técnicas para o fim contrário, deteção de falsificação, é neste contexto essencial. (E12)

Facilidades de rastreamento de trajetórias individuais a partir de dados móveis ou o reconhecimento facial a partir de câmaras urbanas e remote sensing (…), permitem acompanhar as acções de perfis suspeitos. (E12)

Em particular, a presença de câmaras em eventos de grande escala e espaços públicos permite fazer uma vigilância em massa para detetar perigos, combatendo o terrorismo doméstico. Para este fim, a aprendizagem pode recorrer a algoritmos de reconhecimento facial e objetos sensíveis, ou deteção de comportamento suspeito. (E12)

Antecipar ameaças e desmantelar eventos que promovam o planeamento/operacionalização de ataques. (E12)

Facilidades de *remote sensing* (satélite, drones), aliadas a avanços na deteção de perfis, categorização de veículos, e análise de trajetórias, pode permitir acompanhamento eficaz das fronteiras marítimas e terrestres. (E12)

Identificar com sólidos graus de certeza ataques informáticos em parte originados por motivações radicalizadas/terrorista. (E12)

		A deteção (e subsequente intersecção) de veículos autónomos de comportamento suspeito, como carros ou drones, em ambientes domésticos, é essencial dada a crescente utilização destes recursos por grupos terroristas em recentes ataques. (E12)
	Combate a outros crimes (B.5)	Estas tecnologias podem ajudar não só na prevenção do terrorismo, mas sim aplicadas na prevenção de outro tipo de crimes. (E3) (…) a utilização de inteligência artificial para análise de fluxos financeiros suspeitos, deteção de lavagem de dinheiro. (E4) Deteção de padrões invulgares em dados (…) na deteção de transações fraudulentas por entidades bancárias, de telecomunicações, e outras. (E10)
	Outros (B.6)	Redução de probabilidade da iminência desses ataques. (E1) A mais notável talvez seja na predição/previsão de ataques. (E10) Construir um modelo preditivo que determina a probabilidade de, num dado dia e num dado estado, ocorrer um ataque terrorista. (E10) Do ponto de vista de deteção e investigação do terrorismo, a inteligência artificial constitui uma ferramenta particularmente útil. (E11)
Dificuldades (C)	**Enquadramento Legislativo (C.1)**	Eu acho que o nosso enquadramento legislativo cria bastantes entraves ao desenvolvimento tecnológico, tem bastantes crivos, mesmo no próprio acesso aos dados. Atualmente que não há

essas tecnologias, o acesso aos dados é muito restrito e precisa de autorização judicial e essas coisas demoram muito tempo (...) ao se aplicar a um sistema de inteligência artificial teria que se configurar completamente o nossos enquadramento legislativo. (E1)

(...) o que acontece é que eles [Polícia Judiciária] têm as reuniões, estudam o projeto, só que para o porém em prática ele tem de ser testado e para ser testado ele precisa de dados e uma das questões éticas que se levanta é que dados vamos utilizar para testar as previsões, margens de erro, etc. (E1)

Em termos político legais também estamos aquém daquilo que pode ser feito. (E2)

Existe um caminho a percorrer no plano jurídico. (E7)

Por outro lado o RGPD não deixa, está tudo protegido, tudo o que sejam dados pessoais, identificadores eletrónicos, biométricos, está tudo protegido nomeadamente a localização da pessoa é uma coisa protegida. (E9)

É verdade que depois o regulamento também diz que para interesse público é tudo uma exceção….mas o que pode ser considerado de interesse público? (E9)

As forças de segurança poderão não ter acesso aos dados necessários para tirar o máximo partido do potencial da IA (…) no entanto, tem implicações éticas importantes (…) e não creio que seja de fácil resolução. (E10)

	Falta de regulamentação legal. Recentemente foi publicada a Carta Portuguesa de Direitos Humanos na Era Digital, onde se proclama que a utilização da inteligência artificial deve ser orientada pelo respeito dos direitos fundamentais, garantindo um justo equilíbrio entre os princípios da explicabilidade, da segurança, da transparência e da responsabilidade, que atenda às circunstâncias de cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação. Apesar de termos esta Carta e normas infraconstitucionais sectoriais, é claramente insuficiente diante dos perigos e riscos associados a um abuso de inteligência artificial, mesmo que sob a justificação de uma pretensa "segurança" dos cidadãos. (E11) A aplicação de nova regulação à aplicação de IA para fins terroristas é simultaneamente difícil e essencial. (E12)
Direitos, Liberdades e Garantias (C.2)	Sou um bocadinho crítica relativamente a isso, às vantagens que poderíamos ter porque, entre aquela velha balança que se discute sempre nas ciências sociais e também no direito, entre a garantia da segurança e o respeito pelos Direitos, Liberdades e Garantias acho que seria difícil enumerar assim as vantagens sem pensar nos desafios. (E1) Eles também proíbem categoria por raça, diferença social, mas eu não sei até que ponto isso na prática é tão preto no branco. (E1) A questão da expansão, ou seja, da vigilância (…) um sistema de IA aplicado para a prevenção do terrorismo e depois para o erradicar, ele tem que supervisionar um grande número de pessoas, ou seja, a vigilância expande-se, os indivíduos acabam por estar na sua maioria sob controlo e todos são suspeitos (…) o próprio sistema nestas análises de redes, acaba por ligar o indivíduo sob investigação a por exemplo, escutas telefónicas e estamos a ouvir a conversa que ele está a ter com

outra pessoa, automaticamente essa pessoa entra sob escuta policial mesmo que não interesse. (E1)

Os próprios erros e viés dos próprios sistemas de inteligência artificial (…) acredito que reflitam práticas históricas de descriminação e racismo porque vai-se alimentar dados que já estão nas bases policiais e ao serem sub-representados vai sempre influenciar o algoritmo, as correlações e previsões para determinadas franjas populacionais. (E1)

Uma pessoa ser sinalizada e não ter nada a ver com aquilo. (E1)

(…) uma dimensão ética (…) e legal que esbarra com a privacidade de dados. Estes são os principais constrangimentos. (E2)

Depois entramos numa questão complicada, a ideia de policiamento de redes sociais não é em si por em causa a privacidade, a liberdade de expressão, as liberdades e garantias? Seria um equilíbrio difícil de fazer. (E2)

(…) correta utilização da tecnologia e das liberdade, direitos e garantias dos cidadão (…) relativamente à sua privacidade, é um equilíbrio delicado de atingir com esta tecnologias. Exige alguma regulamentação e um olhar atento do legislador e dos vários órgãos de soberania porque há potencial para abuso visto que estas tecnologias permitem vigilância em massa. (E3)

Portugal, há mais de 40 anos felizmente não é um estado autocrático mas nunca sabemos que tipo de regime poderemos vir a ter e estas ferramentas prestam-se muito para a vigilância da população, manipulação e abuso de poder, por isso a sua utilização deve ser regulada de alguma forma para

garantir que é utilizada para os fins de investigação criminal, do combate ao terrorismo, prevenção do crime em geral, mas não permitir que ela seja usada politicamente ou outros fins ilícitos. (E3)

Existe um caso de um terrorista em matou 14 pessoas e acabou por ser morto no Estados Unidos, que tinha um telemóvel da Apple, um IPhone. O FBI queria que a Apple os ajudassem a desbloquear o IPhone para terem acesso e tal não foi possível porque, para eles, a privacidade estava acima de quase tudo. Obviamente que isto é um ponto de vista válido. (E4)

(…) questões de privacidade, podendo estar a ser investigados abusivamente cidadãos pacíficos. (E4)

(…) mas na parte de interceção de comunicações seria tudo mais complicado porque entram questões de privacidade, legalidade, acesso aos dados, sendo preciso a colaboração das empresas que detêm os meios (redes sociais, telemóveis…). (E4)

(...) rapidamente podemos passar de um regime legítimo para um não legítimo (…) Todas essas ferramentas de violações de privacidade foram instaladas com as melhores das intenções para detetar crime, podem passar a ser usadas para controlar cidadãos. Há aqui um equilíbrio muito precário e difícil de obter. (E4)

Questões de privacidade, porque há sempre um equilíbrio difícil entre privacidade, liberdade e segurança. Temos sempre de abdicar um pouco da nossa liberdade em prol da segurança. (E4)

(…) outro desafio é aquilo que hoje é bastante discutido – privacidade. Quando usamos ferramentas destas facilmente podemos perder o controlo da coisa. (E5)

Claro que existe um outro obstáculo que é o da legalidade, ou seja, a possibilidade de fazer estas coisas sem violar os direitos dos outros. (E6)

Acredito que a relação da inteligência artificial e a violação de direitos individuais seja um falso problema, pois estas questões estão a ser discutidas ao mais alto nível político-diplomático e jurídico europeu e o velho continente talvez seja a região do mundo onde exista uma maior preocupação com esta realidade. (…) Neste sentido, a inteligência artificial e outros aspetos do desenvolvimento tecnológico não serão nem deverão ser incompatíveis com direitos, liberdades e garantias. (E7)

(...) até que ponto estamos disponíveis para abdicar da liberdade em prol da segurança? Há certamente um ponto onde a partir do qual abdicamos tanta liberdade que prescindimos da natureza democrática dos nosso regimes e portanto há um equilíbrio dificílimo entre liberdade e segurança. (E8)

Acima de tudo são os limites éticos que estão a impedir a utilização destas ferramentas (…) se olhar para o RGPD a quantidade de limitações que são impostas, e que fazem sentido, porque do ponto de vista de uma pessoa inocente fazem sentido, o preventivo é altamente invasor da privacidade. (E9)

Sobretudo a ver com a privacidade e com o limite porque esse não é fácil, que é estabelecer o que é que é democraticamente aceitável e o que não é porque a IA não sabe fazer isso, portanto eu para ter a capacidade de por exemplo identificar que há um terrorista em Portugal, eu tenho que captar as imagens de toda a gente. (E9)

De um ponto de vista de combate ao terrorismo, dados potencialmente úteis—resultantes de processos de vigilância/monitorização, levantam questões de privacidade não-triviais. (E10)

Os modelos preditivos da IA são baseados tipicamente em dados históricos e sofrem, invariavelmente, de viéses resultantes da atuação humana—com os seus inevitáveis preconceitos, pré-juízos, inconsistências e outros erros. (E10)

Respeito pelos direitos fundamentais. Direitos constitucionalmente consagrados como o direito à dignidade humana, à imagem, à reserva da intimidade da vida privada, à proteção de dados pessoais, à inviolabilidade dos meios de comunicação, não discriminação, ou ainda a liberdade de expressão, liberdade de reunião e o princípio da igualdade. Uma utilização desregrada de inteligência artificial traz consigo o potencial de lesão grave de direitos fundamentais. (E11)

Basta consultar-se a Lei n.º 52/2003, de 22 de Agosto, a Lei n.º 5/2002, de 11 de Janeiro, ou a Lei n.º 109/2009, de 15 de Setembro, para se constatar a ausência de qualquer referência a inteligência artificial. E para que, em casos de investigação de terrorismo, se realize justiça, não é suficiente descobrir-se a verdade material ou histórica dos factos. É necessário que tal aconteça de um modo processualmente válido, em que os direitos fundamentais foram devidamente tomados em consideração. (E11)

Minimizar viés discriminatório na aprendizagem dos modelos, potenciadores de discriminação negativa de inocentes (e.g. baseado em género, etnia, orientação, características físicas, entre outros). (E12)

	Garantir a conformidade com leis e princípios de privacidade. (E12)
Responsabilidade (C.3)	(...) a questão da responsabilidade (…) obtendo um resultado enviesado informado por uma análise errónea, depois de quem é a responsabilidade por conotar determinado indivíduo como suspeito? Será da pessoa que criou o sistema de IA? Quem autorizou a sua implementação na instituição policial? Ou no agente policial que confiou no resultado que o sistema deu? Esta questão preocupa-me muito. (E1) Por exemplo, se nós colocarmos gatos e cães e ensinarmos “isto aqui são gatos” e mostrarmos imagens de gatos e depois “isto são cães” e mostrar fotos de cães, o algoritmo aprende a distinguir gatos de cães, mas nós não sabemos exatamente explicar como (…) Ou seja, como é que depois explicamos a um juíz que este indivíduo foi selecionado por um sistema com base em IA? (E3) No caso das forças policiais, muitas vezes os resultados destas ferramentas são depois utilizados como prova, queremos levar ao juíz uma prova de que aquele indivíduo é suspeito de algo. Quando é necessário um mandado ou em fases de julgamento que é necessário que haja solidez na ferramenta, tal não é fácil. Um dos problemas com que nos deparamos é a chamada *explainability*, ou seja, a inteligência artificial, muitas vez funciona como uma caixa negra. (E3) (…) essas técnicas podem falhar, pelo que qualquer ferramenta de IA deve ter uma pessoa por trás para ver se consegue validar os resultados apresentados e não acreditar cegamento naquilo que aparece. (E6) Quem trabalhe com sistemas desse tipo, tem que estar consciente de que há sempre a possibilidade de algumas das respostas obtidas serem incorretas, e alguma serem mesmo falhas catastróficas.

Sistemas que sejam minimamente interpretáveis são obviamente muito mais confiáveis dado que pode existir a possibilidade de se conseguir saber como se chegou à resposta dada. (E6)

(...) são as ferramentas de IA que se comportam como caixas negras, aquelas que dão respostas sem nenhuma explicação associada à forma como se chega a essas resposta. Infelizmente são essas técnicas que hoje em dia têm mais sucesso e porque isso são as mais utilizadas. (E6)

(…) em momento algum transformar um instrumento de inteligência artificial em meio de prova ou argumento válido para condenações em tribunal. (E8)

Sendo certo que, em momento algum essas ferramentas devem ser utilizadas como meio de prova porque, a existência de padrões em si não constitui crime, ou seja, pode haver um padrão e havendo esse padrão, pode ou não haver radicalização. (E8)

O desafio é este – temos de olhar para a inteligência artificial como uma ferramenta – é essencialmente uma ferramenta e não pode ser mais do que uma ferramenta. Nós não podemos acabar por validar algumas das teorias que a ficção científica desenvolveu (…) de quase se prever o crime, ou seja, de condenar alguém porque conseguimos prever que ela iria cometer um crime (…) Isso faz-se mediante indícios tangíveis. A identificação de padrões e comportamentos online, do meu ponto de vista, nunca poderá constituir um meio de prova para condenação. A inteligência artificial e outras ferramentas tecnológicas devem sim ser um instrumento de auxílio às forças e serviços de segurança e devem funcionar como sistemas de alerta prévio e não mais do que isso. (E8)

(…) as taxas de erro ainda são consideráveis, mesmo que 1% é muito pouco, mas 1% pode tramar a vida de algumas pessoas, centenas ou milhares. (E9)

(...) estas técnicas são cegas, no sentido em que não respeitam limites, nós não temos a capacidade de que as técnicas percebam “eu aqui não posso olhar porque esta pessoa é inocente” (…), têm de ser os humanos a dizer “é isto que é legal e é isto que é ilegal. (E9)

A prova começa a ser uma coisa muito complicada de gerir. (E9)

Tem a ver com a atuação baseada em predições ou inferências realizadas por sistemas—por exemplo, será que as predições produzidas por estes sistemas são admissíveis em tribunal ou evidência suficientemente forte para justificar atuar com base nelas? E, em caso de erro, a quem cabe a responsabilidade da decisão? (E10)

Apesar dos importantes progressos da IA em anos recentes, estes sistemas são ainda falíveis. Tal falibilidade não é, por si só, um problema. O desafio coloca-se devido à “falha catastrófica” deste tipo de sistemas. (E10)

Muitos dos sistemas de IA mais sofisticados sofrem do problema da “caixa preta”: as predições/recomendações produzidas por estes sistemas vêm sem qualquer tipo de justificação, o que torna a adoção desta tecnologia difícil devido à desconfiança dos utilizadores e dificulta o diagnóstico de problemas em situação de falha. (E10)

A sensibilidade e correto isolamento de falsos positivos e falsos negativos é também essencial. (E12)

	Desenvolver processos de regulamentação e certificação para garantir que os sistemas de AI (…) fornecem responsabilidade no caso de uso indevido. (E12)
Investimento (C.4)	(...) recursos financeiros (E3) (…) recursos, capacidade económica. (E5) (…) o facto de muitas entidades portuguesas não terem a capacidade de fornecer este tipo de tecnologia, ou seja, temos de comprar isto no mercado e comprar no mercado acaba por ser uma dependência de terceiros bastante estranha. (E5) Estes recursos quando utilizados são muito caros e portanto, existe aqui um desafio económico comparado com os Estados Unidos ou Israel por exemplo. Não estamos a falar só de custo direto em si na aquisição (…) é preciso comprar licenças, ter formação. É preciso não ter só as pessoas que operam os utilizadores mas, em alguns casos, se queremos manter a independência relativamente aos fornecedores é preciso ter a capacidade de operar, daí apoio tecnológico. (E5) Principalmente a questão económica: deveria haver uma aposta e investimento maior nesta área. (E6) (…) o investimento relativamente reduzido no plano tecnológico, se compararmos com outros países. Mais de 90% do orçamento das Forças e Serviços de Segurança é destinado a despesas com pessoal, restando pouco mais de 5% para investimento. (E7)

	O investimento nestas novas tecnologias tem de ser feito precisamente para garantir e defender os direitos, liberdades e garantias e não contra estes. Se os estados, e em particular as polícias e a justiça, não recorrerem às novas tecnologias na prevenção e combate às formas grandes de criminalidade, ficaremos mais vulneráveis. Se não o fizermos, as nossas sociedades e os Estados de direito poderão ser mais facilmente alvo de ataques por forças que visam destruir os nossos modelos de sociedade: as democracias e o respeito pelos direitos, liberdade e garantias dos cidadãos. (E7) A utilização deste tipo de sistemas implicaria um parque informático relativamente bem apetrechado e um conjunto de sistemas de informação bem organizado e automatizado, sobre o qual seria realizada a implementação desta tecnologia. Não conheço quais as infraestrutura tecnológica actual das forças de segurança, mas atrever-me-ia a sugerir que a sua atualização para suportar este tipo de sistemas poderá requerer um investimento considerável. (E10)
Capacidade Técnica (C.5)	(…) os próprios computadores e os meios que a polícia tem atualmente para suportar esse tipo de ferramentas. (E1) Não há a tecnologia suficiente. (E2) (…) desafios de ordem tecnológica (…) é necessário que a tecnologia tenha uma fiabilidade interessante para que também as polícias confiem na tecnologia e possa ser utilizada com eficácia. (E3) Neste caso, têm que ser as tecnologias mais recentes possíveis. (E4)

	(...) aspetos técnicos, porque vigiar não é fácil e os terroristas fazem os possíveis para se esconderem e não deixarem pistas (…) Portanto, há o desafio de tentar usar a tecnologia de inteligência artificial para analisar grandes volumes de dados – transações financeiras, comunicações de redes sociais e outros para detetar atividades suspeitas. (E4) As Forças e Serviços de Segurança e de Informações deverão melhorar a sua capacidade de TECHINT, ou seja, adquirirem software de Inteligência Artificial. (E7) Dispõe Portugal de capacidade tecnológica para criar soluções deste tipo? (E8) Desenvolver algoritmos e princípios de aprendizagem mais robustos (…) Avanços focais na área da aprendizagem (...) têm menos de 10 anos. É, por isso, expetável que a produção de IA para incitação e combate ao terrorismo ainda esteja longe de atingir o seu auge. (E12)
Gestão de meios humanos (C.6)	A própria realidade das práticas policiais porque há sempre além de tudo uma resistência à mudança por parte dos agentes policiais, principalmente daqueles que têm muitos anos de carreira. (…) Logo aí existe uma desafio (…) porque iria requerer mais formação especializada e prática para os agentes policiais. É verdade que agora com os novos concursos surge uma camada mais jovem com mais conhecimentos nas tecnologias, mas teremos sempre os mais antigos. (E1) A resistência à mudança também nunca é muito confessada pelos agentes policiais (…) uns dizem “sim sim, isso é muito bom”, mas eu não seu até que ponto a ideia de sere substituídos por um software seria assim tão bom e tão bem recebido. (E1)

(…) [o problema] é a muitas vezes a capacidade técnica de utilizar essas ferramentas, ou seja, falta de recursos humanos nas forças policiais para investigação da prova digital. (E3)

Principalmente humanos. Não é tanto recursos para comprar computadores (…) mas meios humanos é principalmente a grande carência que temos neste momento para permitir a aplicação quer a nível da operação, ou seja formação das forças policiais, quer a nível da conceção, manutenção e instalação e fornecimento, ou seja, todo o ecossistema que permite que estas tecnologias passem a ser consideradas produtos. (E3)

(...) que eu saiba, qualquer Força de Segurança, nem em Portugal nem na Europa diz estar equipada para este efeito porque não tem recursos humanos suficientes. Isso é uma carência que existe em Portugal e na Europa, ou seja, face aos aumentos do recurso digital teremos cada vez mais necessidade de recursos humanos que estejam habilitados a realizar a investigação na área digital. (E3)

Muitas vezes são soluções muito *costum* que necessitam de muita engenharia para instalar, o que implica muitos recursos humanos e qualificados nestas áreas que são escassos, quer em Portugal como mundialmente. (E3)

(…) há a necessidade de conhecimentos tecnológicos por parte dos utilizadores. (E3)

Existe um grande caminho a percorrer na área do treino das forças policiais e de recrutamento de recursos especializados para as forças policiais, embora este tipo de recursos sejam altamente procurados nos mercados por isso não é fácil. (E3)

	Neste caso (…) têm que ser pessoas formandas, instalar sistema sofisticado de inteligência artificial para fazer deteção de crime ou combater o terrorismo tem esses obstáculos típicos em Portugal. (E4) (…) *know-how*. (E5) Devemos pensar nas carreiras – temos o exemplo da Polícia Judiciária – esta tem a carreira policial, mas também tem uma carreira técnica, promovendo a abertura de concursos de técnicos para engenharia informática, engenharia geoespacial, etc. Na Polícia de Segurança Pública, devemos pensar em reestruturar a carreira técnica, na medida em que precisaremos de peritos na área ciber (engenheiros, técnicos, etc). Defendo que devemos apostar na formação de Oficiais de Polícia, nomeadamente na frequência de cursos técnicos, mestrados e doutoramentos para os especializar na vertente dos sistemas de informação. Em suma, no médio prazo devem ser recrutados recursos humanos, ser reestruturada a carreira técnica e formar Oficiais de Polícia para robustecerem a estrutura tecnológica da PSP. (E7) Falta de formação das forças de segurança nesta área, ou a pouca integração de especialistas nesta área nessas mesmas forças. (E10)
Ataques informáticos e Uso indevido da IA (C.7)	(...) a segurança dos dados, temos assistido ultimamente a muitos ataques informáticos. A IA come, come dados mas não consegue garantir que os dados não são acedidos por outras entidades e o problema é que os dados da inteligência artificial para fins de policiamento e fins de investigação criminal acabam por ser dados sensíveis de pessoas que já tiveram contacto ou irão ter porque esses sistemas fazem esse tipo de previsões. (E1)

(…) existem algumas fragilidades que é a própria tecnologia ser sujeita a ataques. (E3)

(…) organizações terroristas e de crime organizado podem utilizar estas novas tecnologias como uma oportunidade, pelo que é fundamental a aprovação de legislação e de mecanismos de fiscalização e controlo que protejam os cidadãos. (E7)

Essas ferramentas também já conseguem produzir imagens – *fake news, fake images* (…) é verdade que na maior parte estas coisas tipicamente são feitas para o *show*, mas (…) é possível e portanto com muito esforço de afinação dos parâmetros do algoritmo estas coisas são possíveis hoje em dia. (E9)

Qualquer pessoa com um computador de gama média consegue desenvolver aplicações próprias que utilizam tecnologia de IA relativamente sofisticada. Isto significa que os próprios terroristas têm acesso a este tipo de tecnologia. (E10)

A utilização de IA no combate ao terrorismo pode, pois, fomentar uma espécie de "corrida às armas", em que ambos os lados procuram tirar partido deste tipo de tecnologia para os seus próprios meios. (E10)

Contra-atuar a IA desenvolvida para apoiar o terrorismo com IA superior. (E12)

Desenvolver processos de regulamentação e certificação para garantir que os sistemas de AI estão protegidos contra o uso adverso. (E12)

Cultura de Segurança (C.8)	Temos a ideia de que somos um país de brandos costumes e que não há uma necessidade de nos preocuparmos com isso. (E1) (…) por outro lado não há uma *awareness* suficiente em termos políticos que permita a alavancagem para outras áreas e essencialmente trabalhar a questão securitária numa perspetiva não reativa mas sempre preventiva. (E2) *Awareness*, consciencialização ou falta dela (…) …falta de consciência política deste tipo de situações e depois financiamento depende da consciência política. Não há uma cultura política deste tipo de atuação, ou seja, não há uma cultura de *intelligence* em Portugal, razão pela qual Portugal ser uma país seguro. (E2) Existe um caminho a percorrer (…) no plano da cultura de segurança. (E7) Quem é que tutelaria este tipo de instrumentos? Seria o Ministério da Justiça porque tem competências sobre a Polícia Judiciária e a Polícia Judiciária tem a Unidade de Combate ao Terrorismo? Seria a Presidência do Conselho de Ministros porque depende desta o Sistema de informações da República Portuguesa? Ou seria o Ministro da Administração Interna da qual dependem a PSP e a GNR? A arquitetura do sistema nacional de segurança faz com que não haja uma resposta evidente a esta pergunta. (E8)
Processo de implementação em Portugal (C.9)	Diria que são tipicamente os mesmos [desafios] que há na implementação de qualquer coisa em Portugal. (E4)

		É uma questão de haver vontade política, se um governo quiser aposta nisso consegue. É uma questão de vontade polícia e de querer agilizar esses processos. (E4) Tem que existir alguma burocracia (…) mas tem que ser agilizado porque quando se for implementar, as tecnologias podem já estar obsoletas. (E4) Por causa das burocracias e "capelinhas". Se estes dados estão nas minhas mãos eu não vou abrir acesso a mais ninguém. (E9)
	Características do Sistema (C.10)	Algumas das características associadas a técnicas de inteligência artificial, como por exemplo a opacidade, constituem, para significativa parte da doutrina nacional e internacional, um obstáculo inultrapassável diante da regra de fundamentação e explicabilidade das decisões que afetem direta e individualmente as pessoas. (E11) Persistente falta de transparência e eficácia dúbia da IA. (E12) Promover sistemas de IA justos, éticos, confiáveis, e responsáveis. (E12)
Necessidade de IA (D)	**Eficácia da utilização de IA (D.1)**	(...) eu não sei se termos sistemas de IA nos torna preparados para esse tipo de eventualidade. Porque o que os estudos nos dizem é que ao nível da eficácia prática, esses tipos de sistemas não têm tido os resultados esperados e por isso não sei até que ponto nos tornaria mais aptos para resolver o terrorismo. (E1)

(…) mas ao mesmo tempo há outros softwares de inteligência artificial que foram aplicados em outros estados e não é por isso que se prevê os ataques terroristas, nem em última instância se evitam. (E1)

A aposta na tecnologia não deve implicar um menor investimento na pesquisa junto de fontes humanas. Uma força de segurança de proximidade como a PSP tem um enorme capital de confiança junto dos cidadãos, instituições, universidades, escolas, organizações não governamentais e deverá rentabilizar esse facto, equilibrando o acesso a uma grande diversidade de fontes humanas com a tecnologia, com vista a melhorar a capacidade para identificar potenciais ameaças e riscos. (E7)

Se é eficaz ou não (…) acontece que muitas vezes o terrorismo e sobretudo os indícios de conspiração terrorista acontecem antes de haver indícios de crime, logo não é possível intercetar comunicações se não tenho prova da ocorrência de um crime ou da iminência da ocorrência de um crime. O combate ao terrorismo faz-se muitas vezes antes disto – esse é um problema legal português referente à eficácia da utilização de inteligência artificial. (E8)

As características de Portugal, quer do ponto de vista legislativo, quer do ponto de vista daquilo que é a nossa arquitetura do sistema nacional de segurança fazem com que essa ferramenta não se torne tão eficaz. (E8)

Vamos usar isto para prever radicalização? (…) a radicalização continua muito presencial e portanto ia incidir sobre um pequeno número de casos. (E8)

	Deve ser encontrado um ponto de equilíbrio entre a crença excessiva e obstinada na inteligência artificial, como se de um remédio para todos os males do mundo se tratasse, incluindo o terrorismo, e a proteção absoluta e irrestrita de certos direitos fundamentais, por exemplo, privacidade, desconsiderando o contributo importante que as novas tecnologias podem oferecer para a prevenção e investigação da criminalidade. (E11)
Risco de ameaça em Portugal (D.2)	O facto de não existir terrorismo é uma face de dois gumes. Por um lado é lisonjeiro e presenteiro que estejamos tão bem colocados em termos securitários nos rankings mundiais. (E2) (…) estamos sempre um passo depois (…) como uma situação não acontece, não é necessário trabalhar no assunto. (E2) Ainda recentemente tivemos uma situação aqui [situação do possível ataque evitado no dia 10FEZ022] onde houve bastante sorte relativamente a um possível ataque. É verdade que Portugal não tem tradicionalmente este tipo de ameaça mas nós estamos num espaço global, hoje em dia já são poucos os países que estão totalmente isolados. Fazemos parte da UE, da NATO, partilhamos posições políticas com estes dois o que nos colocam também como potenciais alvos, não só a nível de recrutamento do terrorismo como a nível de ataques. (E3) Não digo que o risco em Portugal seja 0, será possivelmente inferior do que na Alemanha ou França ou Itália mas não será 0. (E3) As pessoas têm a perceção de que não pode acontecer nada mas obviamente que pode. (E4)

	Em Portugal, não temos felizmente tido casos de terrorismo (…) e espero que não continuemos a ter. (E6)
	Alias, isto faz me sempre lembrar a situação que ocorreu há pouco mais de um mês com o aluno da faculdade de ciências. (E6)
	Em Portugal ainda há uma certa tendência para considerar a segurança como um dado adquirido tendo em conta os excelentes indicadores de criminalidade. Desta forma, o poder político não sente a segurança como uma prioridade. (E7)
	É falso de que a ameaça terrorista não existe em Portugal. Existe, tem um nível inferior do que tem em outros locais. (E8)
	É uma boa pergunta, eu fiz-me a mesma pergunta, mas em Portugal há terrorismo? Se eu começar a pensar, não me parece que haja, mas com os novos ataques, ciberataques fazem me perguntar porque é que nos escolheram a nós? Ou porque não nos escolheram? (E9)
Necessidade de IA (D.3)	Agora, será necessário? Eu acho que qualquer desenvolvimento tecnológico pode trazer os seus benefícios, temos é de trabalhar os seus riscos. (E1)
	É fundamental porque em termos doutrinais essa situação tem de ser trabalha e tem que ser bem marcada e definida na PSP. (E2)
	Fundamental! E sublinho fundamental as parcerias público privadas principalmente na gestão de dados. (E2)

(…) por isso acho relevante. (E3)

Acho que é importante, nomeadamente em Portugal, sendo um país seguro, provavelmente um dos mais seguros do mundo. (E4)

Vivemos naquilo que podemos chamar de paradigma digital (…) as comunicações hoje não são feitas por pombos de correio nem sinais de fumo, são através de mensagens digitais usando aquilo a que chamados de internet ou telemóvel e a quantidade de dados que gera é gigantesca. Considerando que o terrorismo é um desafio global, eu acho que é fundamental usarmos aquilo que chamamos de estado de arte das tecnologias no qual se inclui ferramentas de análise sistemática e com inteligência desses dados. É impossível não o fazer. Possível é, é extremamente ineficiente e ineficaz. (E5)

É essencial, hoje não se consegue fazer nada sem isso. (E5)

Mas sob forma de combater o terrorismo em geral e aos dias de hoje, acho que a utilização destas ferramentas é a única forma de o conseguir. (E6)

Se houver o mínimo de noção o do que é uma estratégia de segurança, o facto de nós não termos um risco de ameaça muito elevado deve convidar-nos a fazer o máximo possível para assim continue. (E8)

Há duas maneiras de olhar para isto. Uma é a maneira portuguesa “como não há problema não fazemos anda” outra é a maneira responsável que é olhar para o cenário e dizer “temos uma

	vantagem competitiva (…) Se esta é a nossa circunstância temos uma vantagem e portanto devemos aproveitar (…) para garantir que os níveis de segurança em matéria de combate ao terrorismo se mantenham elevados. (E8) Portanto acho que deviam ter ferramentas (…) acho que é relevante fazer, pelo estar preparado para. (E9) A minha resposta é tendencialmente afirmativa. (E11)
Processo de Implementação de IA (D.4)	Embora sejamos sempre atrasados relativamente a outros países europeus e dos outros continentes, acho que vamos acabar por seguir as tendências, daqui a 20 ou 30 anos, acho que isso acabará por se implementar. Se é necessário? Eu acho que é importante estarmos preparados para uma eventualidade. (E1) É preciso atender aos contextos específicos onde estamos a aplicar, ou seja, seguimos as tendências dos outros países? Sim, mas aqui aplicar, teríamos de adequar primeiro aos nossos OPCS. (E1) Se por outro lado, existe uma proposta de Conselho Europeu para regular a IA em última instância acontecerá como a partilha de dados para fins de investigação criminal. (E1) Sendo um país relativamente seguro, essas ferramentas são provavelmente mais fáceis de implementar porque os comportamentos suspeitos são mais diferentes do que os comuns. Somos um país relativamente homogéneo do ponto de vista sociocultural, não é muito homogéneo, mas mais homogéneo do que países maires comparando com Estados Unidos e França. (E4)

(…) referente aos limites entre segurança e liberdade (…) é muito mais tranquilo porque o sistema é tão garantista que praticamente não existem ameaças à liberdade. (E8)

Podemos ter muita dificuldade em fazer modelos porque se não temos dados, ataques, temos um problema. (…) …provavelmente sim [necessário e eficaz?] mas num nicho que faça sentido por exemplo os ciberataques porque esses só têm tendências a aumentar agora em terrorismo tradicional ou político não me parece (…) no entanto devemos relembrar que a Polícia Judiciária pode ter grandes bases de dados relativamente a ataques que conseguiu prevenir. (E9)