Instituto **S**uperior de **C**iências **P**oliciais e **S**egurança **I**nterna

Mário Rui Gonçalves Pereira

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXIV Curso de Formação de Oficiais de Polícia

O impacto das *Fake News* na segurança e ordem pública

Orientadores:

Superintendente Luís Elias

Superintendente Leitão da Silva

Lisboa, 13 de maio de 2022

Instituto **S**uperior de **C**iências **P**oliciais e **S**egurança **I**nterna

Mário Rui Gonçalves Pereira

Aspirante a Oficial de Polícia

Projeto de Dissertação de Mestrado Integrado em Ciências Policiais

XXXIV Curso de Formação de Oficiais de Polícia

O impacto das *Fake News* na segurança e ordem pública

Orientadores:

Superintendente Luís Elias

Superintendente Leitão da Silva

Estabelecimento de Ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Curso:	XXXIV CFOP
Orientadores:	Superintendente Luís Elias Superintendente Leitão da Silva
Título:	O impacto das *Fake News* na segurança e ordem pública
Autor:	Mário Rui Gonçalves Pereira
Local de Edição:	Lisboa
Data de Edição:	13 de maio de 2022

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 do Superintendente Luis Elias e do Superintendente Leitão da Silva.

Dedicatória

Aos meus pais, à Eduarda e aos meus amigos,

por contribuírem para que esta etapa fosse superada.

Agradecimentos

No findar desta etapa, que é uma das maiores conquistas até agora alcançadas, não poderia deixar de agradecer às pessoas que mais marcaram este meu percurso, e contribuíram direta ou indiretamente para a construção deste trabalho.

Em primeiro lugar, o meu sincero agradecimento ao Superintendente Luís Elias e ao Superintendente Leitão da Silva, por toda a orientação, e por todo o acompanhamento que me deram. Agradecer por todo o apoio e toda a ajuda, e pela disponibilidade e prontidão com que me auxiliaram, e por terem estado presentes durante toda a orientação. A reconhecida experiência profissional aliada ao seu percurso académico constituíram uma forte motivação e desafio para atingir os objetivos propostos com o presente trabalho.

Aos entrevistados, pela disponibilidade, e pela colaboração que prestaram para a consolidação da nossa dissertação, através de todo o conhecimento e sabedoria partilhados. Os cargos e funções desempenhadas e o reconhecido mérito profissional e académico, enriqueceram, de forma inquestionável, a investigação

Ao XXXIV CFOP pelos laços de camaradagem que estabelecemos. Foram cinco anos de alegrias, muitas emoções, e muitas histórias que guardamos para contar. Cinco anos de superações, que nos trouxeram até aqui. Que estes laços criados nunca se percam com os anos.

À minha família, por todo o apoio que sempre me deram, e por estarem sempre lá para mim. Por sempre acreditarem e me motivarem em todos os momentos da minha vida, e por todas as palavras que me ajudaram a chegar onde estou hoje.

Aos "nasciturcios", por todos os momentos de maior cumplicidade e todos os momentos de descontração. Que esta amizade não se perca com os anos e que continuemos, juntos, a criar memórias.

Aos meus amigos do Porto, por todas as lembranças que levo, e todas as recordações incríveis que guardo comigo.

À Eduarda, por ser um dos meus pilares e tornar os meus dias mais fáceis. Por todo o apoio que sempre me dás, pela motivação, pelo carinho, e por todo o amor que me enche o coração.

À minha Mãe, pelo coração de ouro que têm, e por me ter feito na pessoa que sou hoje. Por todos os conselhos, e todas as vezes em que me abriste os olhos, sem que nunca saísse do teu abraço.

Por fim agradecer ao meu Pai, por seres o exemplo de pessoa e de polícia que quero ser. Por nunca hesitares em ajudar-me, e por estares sempre presente. É um orgulho seguir as tuas pisadas.

Resumo

Tal como qualquer fenómeno social, a criminalidade acompanha as mutações que as sociedades comportam. As ameaças híbridas representam uma das maiores preocupações securitárias da atualidade, devido à imprevisibilidade das mesmas, bem como das diversas formas que estas podem assumir, podendo por em causa a segurança e a ordem pública. Neste sentido, as Polícias devem controlar este tipo de ameaças e mitigar os impactos que possam vir a ter. Por sua vez, o desenvolvimento tecnológico potenciou e facilitou a iniciativa de alguns tipos destas ameaças, como as *Fake News.*

O combate às *Fake News* passa pela monotorização e controlo de fontes abertas, no sentido de identificar informações falsas e os seus atores. No entanto, a falha na deteção de *Fake News* pode enviesar a gestão e o planeamento de grandes eventos. Assim, através do ciclo de produção de inteligência, deve ser feito um esforço no sentido de identificar estas informações falaciosas impedindo a sua utilização em relatórios de inteligência policial.

Palavras-chave: Ameaças Híbridas, Desinformação, *Fake News*, Informações, Polícia de Segurança Pública

Abstract

Like any social phenomenon, crime goes hand in hand with the changes that societies undergo. Hybrid threats represent one of today's greatest security concerns due to their unpredictability and the different forms they may take, which may jeopardize security and public order. In this sense, police forces must control this type of threat and mitigate the impacts they may have. In turn, technological development has enhanced and facilitated the initiative of some types of these threats, such as Fake News.

The fight against Fake News involves the monitoring and control of open sources, in order to identify false information and its actors. However, failure to detect Fake News can bias the management and planning of major events. Thus, through the intelligence production cycle, an effort must be made to identify this misleading information and prevent its use in police intelligence reports.

Keywords: Disinformation, Fake News, Hybrid Threats, Information, Public Security Police

Lista de Siglas, Acrónimos e Abreviaturas

AIP	Área de Interesse Permanente
CCPECE	Comunicação Conjunta ao Parlamento Europeu ao Concelho Europeu
COMETLIS	Comando Metropolitano de Lisboa
CPI	Ciclo de Produção de Inteligência
CRP	Constituição da República portuguesa
DN	Direção Nacional
EUROPOL	Agência da União Europeia para a Cooperação Policial
HUMINT	Human Intelligence
IA	Inteligência Artificial
IDITESDE	Instituto para o Desenvolvimento de Inteligência no Âmbito do Terrorismo Segurança e Defesa
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
IMINT	Imagery Intelligence
MASINT	Measurements and Signatures Intelligence
NATO	North Altantic Treaty Organization
NEP	Norma de Execução Permanente
OCS	Órgão de Comunicação Social
OSINT	Open Sources Intelligence
PROTINT	Protected Information Intelligence
PSP	Polícia de Segurança Pública
SIGINT	Signals Intelligence
SINTEL	Sistema de Inteligência Policial

SOCMINT	Social Media Intelligence
UE	União Europeia
U.r.	Unidade de Registo

Índice

Índice de Figuras

Introdução

Os fins de qualquer Estado de direito democrático passam pela garantia da segurança, da justiça e do bem-estar dos seus cidadãos, conforme afirma Clemente (2015). Neste sentido, realçamos a necessidade de garantir as condições essenciais para que se promovam estes princípios, priorizando a adoção de políticas de segurança adequadas e eficazes.

Por sua vez, a Constituição da República Portuguesa estabelece um conjunto de direitos fundamentais atribuídos a todo e qualquer cidadão, nomeadamente o direito à liberdade e à segurança, consagrado no artigo 27.º, que estabelece logo no n. º1 que "todos têm direito à liberdade e à segurança". Assim, e uma vez que a segurança se constitui como uma das prioridades de um Estado, é necessário que haja uma constante adaptação por parte dos promotores de segurança, nomeadamente das Polícias, a todas e quaisquer ameaças, tradicionais, e não convencionais.

A atualidade e a capacidade de mutação e mobilização das ameaças híbridas constituem uma das maiores preocupações em termos securitários para todos os atores estatais. A NATO (North Atlantic Treaty Organization) (2010, como citado em Larsen & Lasconjarias, 2015) explica que ameaças híbridas são caraterizadas pela capacidade de eficazmente empregar meios convencionais e não convencionais de forma adaptável e com um intuito de prosseguir um determinado fim, podendo este estar diretamente relacionado com ameaças à segurança interna e externa de um Estado.

Verificamos a necessidade de cada vez mais serem reforçadas e implementadas políticas de cooperação internacionais, de modo a gerar fluxos de partilha de informações e experiências no combate a este novo tipo de ameaças, facilitando assim a resposta às mesmas, e possibilitando que sejam mitigadas eventuais consequências. De acordo com Treverton et al. (2018) e uma vez que o leque das ameaças híbridas é bastante vasto, optamos por explorar a problemática da desinformação associada às *Fake News*.

Apesar das *Fake News* não serem um fenómeno recente, denotamos que a crescente mediatização deste fenómeno no seio público, tem gerado um conjunto de implicações para a vida em sociedade, podendo estas ter uma interferência direta ou indireta. Por sua vez, o desenvolvimento tecnológico abriu um conjunto de novos horizontes e possibilidades que

outrora não existiam, derivadas das potencialidades dos meios tecnológicos. O livre acesso a aplicações e plataformas permitiu a partilha deliberada de um conjunto de informações sobre as quais muitas das vezes existe a impossibilidade de garantir a sua veracidade. Assim, vivemos em sociedades que, apesar da maior disponibilidade de informação que encontrem, poderão não ser as mais informadas. A partilha de desinformação, constitui um dos maiores perigos aliados à revolução tecnológica, uma vez que impele nos seus utilizadores um falso sentimento de verdade.

Os estudos científicos em torno das *fake news* estão hoje muito associados às áreas das relações internacionais, defesa e *intelligence*. Contudo, não se podem desassociar as ciências policias tendo em consideração o impacto que as mesmas podem ter na segurança e ordem pública.

Com o desenvolvimento do nosso estudo, pretendemos perceber e determinar quais são os possíveis impactos das *Fake News* na segurança e na ordem pública, e averiguar as potenciais formas de mitigar estes mesmos impactos, sejam eles diretos ou indiretos. Neste sentido, foi definido como objetivo principal do nosso estudo determinar o impacto das *Fake News* na segurança e ordem pública. Deste objetivo principal derivou um objetivo especifico que consiste em perceber se existe alguma forma de impedir estas ameaças e mitigar as suas possíveis consequências.

O primeiro capítulo da nossa dissertação tem como objetivo expor o estado da arte existente relativamente às ameaças híbridas, de modo a concetualizar estas ameaças e perceber os impactos securitários associados às mesmas. Ainda neste capítulo é realizada uma abordagem às *Fake News*, através da sua concetualização e do estudo da evolução histórica deste fenómeno. Por último abordamos alguns dos mecanismos de deteção de eventuais *Fake News* que existem e alguns métodos mais convencionais de deteção.

No segundo capítulo, é feita uma abordagem ao papel do ciclo de produção de inteligência, de onde partimos de uma abordagem ao conceito de inteligência. Posteriormente, é realizado um enquadramento do ciclo de produção de inteligência e das fontes de inteligência, estabelecendo-se um paralelismo com a atividade da Polícia de Segurança Pública neste setor, através da análise de documentos estratégicos. Ainda, e no sentido de aprofundar o estudo do impacto das *Fake News*, optamos pela exposição de algumas das dificuldades inerentes à

preparação das operações planeadas, visto que dentro da tipologia das operações, estas constituem o tipo de operações que sofrem um maior impacto com a falha na deteção de eventuais *Fake News*, ou com a gestão da desinformação.

O terceiro capítulo diz respeito ao método onde exploramos as escolhas metodológicas da nossa dissertação, explicando os procedimentos adotados na utilização e tratamento das entrevistas no quarto capítulo. No quinto capítulo, é feita a análise e discussão dos resultados obtidos, utilizados para a conclusão do nosso estudo.

Neste seguimento, e de acordo Quivy e Campenhoudt (2017), durante uma investigação deve ser definido, numa primeira fase, um fio condutor que delineie toda a investigação científica, do qual resultará uma pergunta de partida que deverá respeitar um conjunto de critérios. Por consequente, os mesmos autores defendem que a formulação de uma problemática inicial possibilita a estruturação de um trabalho coerente (Quivy & Campenhoudt, 2017, p. 32). Deste modo, a nossa investigação terá em conta o seguinte problema:

- Qual o impacto das *Fake News* na segurança e na ordem pública?

Capítulo I – Ameaças Híbridas

1.1- Definição e conceptualização

A crescente mediatização do impacto securitário das ameaças híbridas tem gerado um conjunto de inquietações na arena pública. Para Castells (2012), as sociedades são um produto que "resulta da interação real entre os modos de produção e os de desenvolvimento estabelecidos e defendidos pelos atores sociais, de formas imprevisíveis, na infraestrutura repressora da história passada e nas condições atuais de desenvolvimento tecnológico e económico" (p. 54). Deste ponto de partida, podemos concluir que as sociedades são constantemente mutáveis, pelo que, de igual forma, podemos afirmar que as mudanças de paradigmas sociais e securitários as acompanham.

O sentimento de insegurança social é um conceito imagético criado pelas próprias sociedades (Bauman, 2006) uma vez que atualmente vivemos nas sociedades mais seguras que alguma vez existiram. Contudo, o facto de vivermos em sociedades cada vez mais seguras, não descarta a possibilidade de exposição a novas ameaças, que possam implicar direta ou indiretamente com a garantia da segurança.

Neste sentido, os atuais desafios à segurança dos Estados passam, numa primeira fase, pela dificuldade de reconhecimento da ameaça e do grau das mesmas (Treverton, 2018). Bachman e Gunneriusson (2015) defendem que as ameaças híbridas se caracterizam pela capacidade de eficazmente empregar meios convencionais e não convencionais de forma adaptável, com um intuito de prosseguir um fim. Por este motivo, estas ameaças apresentam-se como um dos principais desafios na prevenção e combate à insegurança global, necessitando de uma intervenção conjunta por parte das Forças e Serviços de Segurança e das Forças Armadas (Corbe & Cusumano, 2018).

As ameaças híbridas incorporam uma nova forma de guerra, que "inclui capacidades convencionais, táticas e formações irregulares, atos terroristas com recurso a violência e coerção indiscriminadas e desordem criminosa, conduzida por ambos os lados e uma variedade de atores não estatais" (Hoffman, 2007, como citado em Freedman, Gjorv & Razakamaharavo, 2020, p. 45). Para estes autores, os métodos não militares das guerras híbridas passam, essencialmente

por campanhas de desinformação e de ciberataques com um objetivo de causar desordem e destabilizar as sociedades, sendo este último ponto uma característica fulcral para a conceptualização de ameaça híbrida. Treverton et al. (2018) explicam que estas ameaças têm em vista o alcance de resultados, sem a necessidade de existir uma guerra real, almejando a desordem social, em particular nos Estados de direito democráticos.

Nesta linha de pensamento, Andersson e Tardy (2015, como citado em Pereira, 2018, p. 9) defendem que "poderá afirmar-se que o que contribui para definir o conceito de ameaça híbrida reside precisamente na natureza variada e difusa das ameaças utilizadas, unidas pela cúpula de um objetivo comum e usadas de forma sistemática". Deste modo, Pereira (2018, p. 9) conclui que não será única e exclusivamente a concretização de uma ameaça um fator fundamental para a determinação das ameaças híbridas, ao invés de que deve ser pela verificação de um conjunto sistemático de ameaças, "pelos mesmos perpetradores, na prossecução de um objetivo específico.".

A natureza do ambiente securitário europeu está a tornar-se cada vez mais híbrido, afirma Sari (2020). Este esclarece que, para além do domínio militar tradicional, as atuais ameaças à segurança estão a difundir-se para todos os aspetos da vida social. Destarte, o autor reforça que os Estados são ameaçados por diversos atores que estão mais predispostos do que nunca a ameaçar a segurança, utilizando, para tal, múltiplas ferramentas não tradicionais de modo a concretizar os seus interesses.

Conforme exposto na Comunicação Conjunta ao Parlamento Europeu, ao Conselho Europeu e ao Conselho (CCPECE) (2018) sob epígrafe, aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas, verificamos a importância que é atribuída às atividades híbridas de intervenientes estatais e não estatais que continuam a representar uma ameaça grave e premente para a UE e os Estados-Membros.

Bachmann e Gunerisusson (2014, p. 3) definem uma Ameaça Híbrida como "multimodal, de baixa intensidade, cinética, ou não cinética, caracterizada por ameaças à paz e segurança internacionais,". Estas assumem várias formas de expressão, como por exemplo as *cyber wars*, o terrorismo e a criminalidade internacional altamente organizada. Não obstante, estes autores associam a estas ameaças um conjunto de desafios, defendidos de igual modo pela União Europeia nas suas estratégias de combate às ameaças híbridas.

Outros autores como Cormac e Aldrich (2018) rejeitam designar as ameaças híbridas como uma categoria analítica e enganosa. Para estes autores, as ameaças híbridas não se sintetizam exclusivamente através de formas de desinformação, podendo estas surgir de diversas maneiras.

Por se tratar de um conceito bastante recente, a doutrina diverge bastante na sua definição. Ainda não podemos precisar uma definição conceptual de ameaças híbridas, contudo, as características mais associadas a estas ameaças passam pela sua natureza variada destas ameaças com o propósito de alcançar um objetivo comum.

A imprevisibilidade de prevenção deste novo tipo de ameaças deve-se a um conjunto de vários fatores, conforme temos vindo a referir. À semelhança da dificuldade de deteção, estas ameaças possuem uma vasta aplicabilidade, nomeadamente a utilização de campanhas de desinformação levadas a cabo por atores estatais e não estatais, com o intuito de reforçar as suas posições políticas, ou com o propósito de influenciar políticas externas de segurança.

É um facto que as ameaças híbridas podem causar efeitos geopolíticos significativos ao nível regional ou mesmo global (Consentino, 2020, p. 1). Através da análise de certos fenómenos recentes, conseguimos ver o impacto que estas ameaças podem gerar e a instabilidade social e política que delas derivam.

Consentino (2020) introduz a teoria da *Post-Truth*, (a teoria da pós verdade). Em traços gerais, e através de certos fatores conducentes a esta teoria, como as mudanças no seio dos órgãos de comunicação social (OCS) e a hibridização da informação, esta teoria fundamenta-se no suporte dos argumentos e das emoções com provas fundamentadas. Contudo, e por se verificar uma enorme dificuldade de distinguir o que é verdade do que é falso, podemos estar a criar convicções incorretas sobre os mais diversos assuntos. Para este autor, vivemos num mundo que, por ser operado fundamentalmente por meios de comunicação social e redes sociais, está a tomar cada vez mais contornos distópicos.

Torna-se crucial entender o fenómeno que se encontra por detrás destas ameaças, perceber o modo como se concretizam, identificar os seus atores, e identificar o impacto e a influência que estas podem ter na vida social. Tão importante como detetar e prevenir estas ameaças é perceber quais as origens das mesmas e os objetivos que estas visam.

De acordo com o Instituto para o Desenvolvimento de Inteligência no âmbito do Terrorismo, Segurança e Defesa (IDITESDE) (2021), o combate à desinformação deve ser feito através de duas vertentes. A primeira, conforme referimos anteriormente, passa pela compreensão dos fenómenos que decorrem na esfera da informação, o impacto da informação, e o impacto que esta informação provoca em diversas audiências. O segundo passa por fornecer uma resposta estratégica para este fenómeno, utilizando novos métodos, novas técnicas e novas ferramentas de combate a estas ameaças. Não obstante, analisar o impacto securitário que estas ameaças podem alcançar é fulcral para perceber o modo através do qual deveremos intervir sobres as mesmas.

1.2- Impacto Securitário das Ameaças Híbridas

Para Nagasako (2020, p. 2), o ciberespaço já é reconhecido como um campo de batalha, em que cada Estado incorpora meios tecnológicos nas suas estratégias militares. Para este autor, surgem então as denominadas *Hybrid Wars*, (as Guerras Híbridas). O impacto destas guerras está ainda aliado à dificuldade de perceber se "existe efetivamente uma ameaça real ou não ".

A utilização de meios como a desinformação, nomeadamente sob a forma de *Fake News*, impossibilita muitas das vezes a identificação de um individuo ou de um Estado enquanto fonte da ameaça, podendo promover e criar climas de instabilidade social e política em certos Estados.

Pelos motivos supramencionados, estas ameaças são difíceis de prevenir única e exclusivamente através de estratégias de dissuasão. Podemos afirmar que vivemos "num mundo cada vez mais interligado e com um ambiente de segurança multipolar" (Vasconcelos, 2009, p. 5), pelo que o desenvolvimento contribui em grande parte para a democratização dos meios de violência. Deixamos de verificar tipos de violência exclusivamente físicos, para registarmos ameaças cada vez mais imprevisíveis e indetetáveis.

Numa era em que a Informação é sinónimo de poder, e o poder, por sua vez, é sinónimo de superioridade, todos procuraram rodear-se do máximo de informação que encontrem ao seu dispor. É precisamente por isto mesmo que a indução de circulação de notícias falsas nos meios de busca e de procura de informações pode ser algo potencialmente perigoso.

Os esforços de combate às ameaças híbridas, no caso concreto, o combate à desinformação, devem ser apoiados por redes de capacidade de deteção precoce de fontes maliciosas, quer sejam em ambiente interno ou externo aos Estados. O próprio programa da União Europeia de Combate às Ameaças Híbridas, a CCPECE (2018), prevê uma forte cultura de cooperação entre Estados Membros, para que estes partilhem fluxos de informações pertinentes para mitigar estes potenciais danos provocados pela desinformação.

Farinelli (2021) esclarece que, apesar das campanhas de desinformação não serem suficientemente poderosas ao ponto de levar pessoas a cometer atos extremistas, estas podem ser tentadoras e capazes de ludibriar, alimentando ideais políticos extremistas. A alimentação deste tipo de ideais pode começar a criar grupos populares extremistas com cada vez maior expressão e adesão, podendo estes, *à posteriori*, provocar problemas à segurança pública., como parece ter sido o caso dos milhares de manifestantes que invadiram o Capitólio em Washington em 6 de janeiro de 2021 e que, alegadamente, foram manipulados por teorias de conspiração e desinformação.

Para Corbe e Cusumano (2018), estas Estratégias de desestabilização política são vulnerabilidades específicas de certos Estados e adaptam-se facilmente ao seio de onde são inseridos. Assumindo que as crises políticas são um dos principais fatores na origem de descontentamento e instabilidade social, podemos então constatar que a criação intencional de instabilidade e a propagação de informações que originem ideais políticos falsos pode dar azo a conflitos ou movimentos sociais.

De acordo com a CCPECE (2018), a desinformação é de facto um fator prejudicial à democracia dos Estados, provocando a erosão da confiança pública nas instituições governamentais e o ataque aos valores fundamentais das sociedades. A capacidade de partilha de informações a uma escala e a um ritmo nunca antes vistos, com um direcionamento específico, permite semear a desconfiança e criar um conjunto de tensões sociais.

O IDITESDE (2021) destaca uma luta constante na disseminação de ideias distorcidas, ou não, que leva à consolidação de falsas perceções e à construção de uma versão manipuladora da realidade e dos factos que a compõem.

Não obstante o impacto perigoso ao nível político e social, a manifestação de ameaças híbridas, conforme exploramos neste capítulo, pode assumir muitas outras formas, nomeadamente através do terrorismo. De acordo com Elias (2019), o terrorismo continua a ser uma das maiores ameaças à integridade dos Estados no século XXI. A propagação de informações tendenciosas e a propaganda terrorista é um dos maiores perigos à integridade e à soberania dos Estados, uma vez que estas circunstâncias promovem a radicalização de indivíduos ou grupos mais permeáveis e geram um grande clima de insegurança na população.

Ainda de acordo com a CCPECE (2018), os esforços para combater e responder às ameaças híbridas devem ser apoiados por uma capacidade de deteção precoce de fontes e atividades híbridas maliciosas, internas e externas, e de conhecimento das eventuais ligações entre acontecimentos muitas vezes aparentemente não relacionados. Para o efeito, é essencial utilizar todos os fluxos de dados disponíveis, incluindo informações de fontes abertas. Ao fazermos recurso a estas fontes, como é de esperar, estamos sujeitos a encontrar um grande fluxo de informações que não são verídicas.

Assim, importa perceber e conceptualizar o papel da desinformação enquanto ameaça híbrida, e perceber a forma como este problema tem evoluído nas sociedades. Por último, importa ainda compreender e determinar eventuais soluções para que se consiga evitar e mitigar este tipo de ameaças.

1.3- A Desinformação: o fenómeno das *Fake News*

1.3.1- Conceptualização

O conceito de desinformação, que tem surgido cada vez mais com frequência em debate público, não é um conceito propriamente novo. De acordo com Ribeiro (2021), a emergência deste conceito é usualmente associada à propaganda negra utilizada durante a Guerra Fria, que consistia em ocultar a verdadeira identidade dos emissores de informação. O mesmo autor afirma ainda que, a par do aparecimento desta nova formulação do conceito de desinformação, a segunda metade do século XX ficou marcada pela promoção de inúmeras campanhas de desinformação, produzidas em larga escala pelos serviços secretos, quer soviéticos, quer norte--americanos.

De acordo com Guess e Lyons (2020) e Vasu et al. (2018), este conceito pode ser definido de duas formas: a informação que é falsa, mas não é criada com a intenção de produzir quaisquer danos designada por *Misinformation*, e a informação que é criada com um único propósito de prejudicar uma pessoa, grupo social ou organização, como são exemplo as *Fake News*. Wardle e Derakshan (2017) corroboram esta teoria e acrescentam ainda uma terceira tipologia de desinformação, a *Mal-information*. Esta tipologia surge da partilha de informação com uma origem de veracidade, com o intuito de provocar danos a terceiros. Um exemplo comum deste tipo de *Mal-information* são os *leaks*, ou fugas de informação. Estas consistem na partilha de uma informação da esfera privada ou reservada, para o espaço público, sem ter sido ainda revelada pela instituição visada.

Existem vários tipos de desinformação e, ao contrário do que se possa pensar, a desinformação não é representada unicamente através de *Fake News*, ou de declarações escritas. Fallis (2015) admite que, apesar de uma grande parte da desinformação passar por declarações escritas, existem outras formas de divulgar imagens falsas, construídas em programas de computação. Quando estas são desenvolvidas por profissionais, torna-se bastante árduo o trabalho de averiguar e verificar se as imagens são de facto verdadeiras, pelo que estas podem ser utilizadas para induzir mais facilmente o erro, desacreditando pessoas, instituições ou países.

Atualmente, e tendo em consideração a maior acessibilidade das pessoas a meios de informação, existe uma maior facilidade de disseminar informação falaciosa através destes mesmos meios. O desenvolvimento tecnológico permite uma maior facilidade em produzir e publicar quaisquer tipos de informação *online*, a qual pode chegar a um elevado número de pessoas. A disponibilidade de um maior número de conteúdos informacionais possibilitou uma mudança da "era em que os cidadãos procuravam informação, quer fosse nos jornais, na rádio, na televisão ou mesmo *online*, para uma era em que a informação vai ao seu encontro" (Ribeiro, 2021, p. 31), o que induz um conjunto de novas dinâmicas no processo de persuasão e indução dos cidadãos.

Altheide e Snow (1979) afirmam que as *Fake News* circulam mais rapidamente nas plataformas sociais que outros tipos de informação. Um estudo levado a cabo por Vosoughi et al. (2018), que incidiu sobre os padrões de difusão de histórias publicadas na rede social *Twitter*,

concluiu que as *Fake News* chegam significativamente mais longe, de modo mais rápido e circulam mais amplamente do que a própria verdade.

Se estas informações se disseminam de forma mais rápida e impactante que as próprias informações verídicas, as *Fake News* podem ter consequências negativas a vários níveis da sociedade, dependendo do tipo do seu conteúdo. Ribeiro (2021, p. 28) constata que o objetivo dos mecanismos de desinformação não é o de levar "necessariamente o público a acreditar em informações falsas, mas antes o de acentuar divisões". Deste modo, ao acentuarmos divisões na opinião pública, estamos a fomentar um clima de incerteza em que os cidadãos deixam de conseguir discernir em que informação confiar.

A 10ª Edição do Artigo de Informação Digital da Instituição Reuters elaborada por Newman et al. (2021) conclui que em Portugal os órgãos de comunicação social continuam a ter uma elevada taxa de confiança, inclusive durante a situação pandémica, que propulsionou a difusão de diversas *Fake News*. Não obstante, este estudo demonstrou que em Portugal se faz bastante recurso às redes sociais com o intuito único e exclusivo de procura de informação. Da análise à rede social *Facebook*, percebeu-se que dos 73% de utilizadores da rede social, 48% utiliza este meio como meio de pesquisa de notícias. Esta rede social é a que demonstra um valor mais significativo na procura de notícias, seguindo-se o *Whatsapp* e o *Youtube* com 21% e 20%, respetivamente.

Conforme podemos constatar, as redes sociais possuem bastante representatividade no que diz respeito à procura de informação. Tal significa que, ao invés de se consultarem conteúdos analisados e publicados por especialistas, as pessoas estão involuntariamente a consumir notícias e informações selecionadas por conjuntos de algoritmos das aplicações que consultam para a procura de conteúdos.

A desinformação pode ter diversos fins. A propaganda utiliza frequentemente a desinformação para iludir os destinatários finais da mensagem. Ainda que não exista uma definição consensual de propaganda, Jowett e O`Donnel, (2014) caracterizam este conceito como a tentativa deliberada e sistemática de moldar perceções, manipular cognições e direcionar comportamentos. É através desta estratégia que imensos países interferem e procuram

influenciar diretamente o público ao nível regional ou global nos planos político e socioeconómico.

Natalie Nougayrède (2018) do jornal *The Guardian* defende que o uso da propaganda já é bastante antigo, mas que, contrariamente ao que se verificava no passado, o desenvolvimento tecnológico permitiu difundir estas campanhas com uma eficácia muito superior. Ao longo da notícia, a jornalista faz menção a diversos casos mediáticos em que foi possível identificar o uso de propaganda pelos OCS, como o caso do Brexit e o caso da influência Russa nas eleições dos Estados Unidos da América e, acrescentamos nós, na atual situação de guerra na Ucrânia em que, quer a Federação Russa, quer a Ucrânia utilizam diversas técnicas de disseminação de propaganda e de desinformação.

Tandoc et al. (2017) defendem que a digitalização das notícias veio desafiar a tradicional definição de notícias. Estes autores referem que a disponibilização de plataformas online proporcionou espaço para que qualquer pessoa, jornalista ou não, pudesse atingir uma audiência em massa.

De acordo com o artigo publicado por Gottfried e Sheaper (2016), seis em cada dez americanos utilizam as redes sociais como meio de pesquisa de notícias. Tandoc et al. (2017), reforçam também a ideia de que as redes sociais, para além do público que atingem, são facilitadores de intercâmbio e de trocas de informação. Contudo, e como já pudemos verificar anteriormente, esta facilitação de difusão de informação nem sempre é benéfica, uma vez que muitos conteúdos partilhados não são certificados, podendo dar azo à disseminação de *Fake News*.

No entanto, existem autores que vão mais além na definição de *Fake News*. Para Van de Weert et al. (2020), as *Fake News* são informações falsas que são associadas a informações de natureza sensacionalista, reproduzindo, muitas das vezes, informações dos OCS.

Para Korta (2018), as *Fake News* assumem-se como uma das principais formas de desinformação. Para este mesmo autor, o termo *Fake New* é sinónimo de uma notícia falsa que tenha um propósito de perpetuar boatos e gerar desinformação, podendo estas informações estar concebidas de modo a se assemelharem a informações verosímeis, despertando assim a atenção de quem as lê.

Esta desinformação assenta na partilha e criação deliberada de informações conhecidas *à priori* como falsas (Wardle, 2017, como citado em Tandoc et al., 2017). Entendemos que um dos propósitos das *Fake News* ou das notícias potencialmente falsas passa por disseminar boatos e informações, que podem culminar em alterações à vida em sociedade, nomeadamente ao nível da ordem e segurança pública.

A necessidade de obtenção de informação é uma das prioridades estratégicas da Polícia, pelo que esta não pode ignorá-la, devendo proceder à sua análise e tratamento. As fontes de obtenção de informação são cada vez mais vastas e acessíveis a qualquer um, pelo que existe ao nosso dispor um conjunto de diversos modos de obtenção de inteligência, nomeadamente através das relações humanas (HUMINT), através de meios técnicos (TECHINT), ou através das várias fontes abertas (OSINT).

A monotorização permanente de dados deve ser uma preocupação das Polícias, uma vez que caminhamos para modelos de decisão cada vez mais fundamentados pelas informações (Ratcliff, 2008). Conforme pudemos constatar, a escolha das informações deve ser criteriosa, para que a tomada de decisão seja a melhor possível.

O propósito da identificação prévia deste tipo de fenómenos possibilita, de acordo com Shu e Liu (2019), a emissão de alertas durante o processo de divulgação das *Fake News*, para que se possam implementar medidas que impeçam a sua propagação pelas diversas vias disponíveis, nomeadamente os meios de comunicação social e as redes sociais.

1.3.2. Evolução do problema

De forma a retratar a evolução de um problema, devemos procurar perceber a sua origem, e enquadrá-lo numa perspetiva histórica. Embora o conceito de *Fake News*, seja bastante recente, podemos analisar a evolução da desinformação, com o intuito de estabelecer um paralelismo com as *Fake News*.

Desde a antiguidade que se procura implementar estratégias assentes na arte de iludir os rivais ou inimigos. Sun-Tzu, considerado um dos pais da estratégia, na sua obra "A Arte da

Guerra" refere que "a suprema habilidade consiste em subjugar os inimigos sem ter que lutar". Refere ainda que "quando prontos para atacar, devemos parecer incapazes de o fazer; quando em movimento, devemos parecer inativos; quando próximos, devemos levar o inimigo acreditar que estamos longe; quando longe, levá-lo a crer que estamos perto" (Tzu, 2015, p. 11). Toda esta estratégia procura identificar formas de iludir os adversários através da desinformação.

O´Shaughnessy (2020) afirma que no mundo antigo a desinformação sempre foi uma arma bastante poderosa e frequentemente utilizada. O autor reforça ainda que a toxicidade e influência desta ameaça tem vindo a crescer uma vez que o mundo é impulsionado pelo desenvolvimento tecnológico, desenvolvimento este que potencia a disseminação de desinformação.

Para autores como O´Shaughnessy (2020) e Ribeiro (2021), o grande fenómeno que marcou a desinformação foram as duas Grandes Guerras mundiais e, consequentemente, a Guerra Fria. Uma das bases da campanha Nazi na segunda Grande Guerra foi assente, precisamente, na criação de falsa propaganda para que conseguissem obter o poder suficiente para iniciar uma guerra, tendo forjado diversos episódios que levassem o povo alemão a acreditar que estavam sob ameaça e se deveriam juntar e apoiar a investida Nazi.

A mobilização bem-sucedida das massas no contexto de conflitos sociais deve-se essencialmente ao facto de existir um conjunto de líderes demagógicos que se aproveitam da utilização e da circulação de informações falaciosas e a fé em crenças impostas, refere Peterson (2020). O caso suprarreferido é um exemplo perfeito de mobilização de massas a um nível macro, onde um líder Nazi conseguiu unir uma nação e promover que essa mesma se envolvesse em atos extremos, nomeadamente o recurso à violência e a repressão de grupos étnicos e religiosos (judeus e pessoas de etnia *romani*) e outras minorias (homossexuais) sob a crença de que eram prejudiciais para o Estado e povo alemão. Este exemplo retrata a facilidade com que se alcançou uma mobilização em massa através do uso de propaganda falsa.

Assim, conseguimos perceber a verdadeira força da desinformação. Com a utilização de estratégias de propaganda, a desinformação deixa de ser uma ferramenta meramente de influência política e/ou social, e passa a ser uma forma de obtenção de poder. Compreendemos que da mesma maneira que o início da Guerra teve por base campanhas de propaganda falaciosa,

podemos inferir que as campanhas de propaganda com base na manipulação da informação podem constituir problemas associados à garantia da segurança e da ordem pública dos Estados.

Através das convenções da União Europeia referentes ao combate às ameaças híbridas, entendemos que esta ameaça tem vindo a ganhar um crescente relevo em termos securitários num mundo contemporâneo cada vez mais em rede. Ainda, a existência de diversas formas de manifestação de desinformação proporciona a facilidade de manipular comportamentos.

Shu et al. (2020) consideram que o problema associado à desinformação tem atraído cada vez mais a atenção da esfera pública. Atualmente, a abertura e o anonimato que as redes sociais fornecem dá azo à difusão de informação falaciosa para inúmeros círculos de pessoas, dificultando a diferenciação da informação credível e não credível.

De facto, Bouças et al. (2020, p. 3) afirmam que o "desenvolvimento tecnológico, que vivemos nos últimos trinta anos, permitiu a multiplicação e profusão de fontes de informação, minimizando a influência dos meios tradicionais de comunicação". Tal facto, permite que narrativas com objetivos difusos ganhem protagonismo no meio social. Os autores defendem ainda que o "desenvolvimento exponencial do ambiente digital, associado à difusão em massa de informação, incrementou de forma incontrolável a difusão de desinformação" (p. 3) e os efeitos em cadeia em termos políticos, económicos, sociais e culturais.

Na teoria, Bouças et al. (2020, p. 3), defendem que o "indivíduo pode produzir uma *fake news*, bastando para isso ter os meios tecnológicos necessários e o conhecimento suficiente sobre o emprego desses recursos". Esta facilidade retratada demonstra efetivamente o verdadeiro grau de perigosidade da ameaça.

Jowett e O`Donnell (2015, p. 394) atribuem um grande enfoque ao papel da *Internet* como "difusora de mensagens de propaganda, referindo que existe uma maior dificuldade dos meios políticos dos Estados de direito democráticos controlarem o tipo de informações que são partilhadas sobre os mesmos", devido a princípios fundamentais como a liberdade de expressão e de opinião. Nas redes sociais, existe uma maior facilidade de partilhar e disseminar informações erradas que possam prejudicar a imagem de partidos políticos e dos seus opositores. Neste sentido, é essencial garantir a verificação de conteúdos com o intuito de detetar e colocar

em causa a manipulação da verdade promovida por regimes autoritários ou grupos que professem teorias da conspiração e desinformação.

Estes autores afirmam ainda que a perigosidade deste fenómeno já levou alguns Estados onde existem inúmeras restrições a direitos, liberdades e garantias, nomeadamente a China, o Irão, a Coreia do Norte e mais recentemente a Rússia, a bloquearem o acesso ilimitado a redes sociais como o Twitter, sobretudo tendo por objetivo a manutenção dos regimes. Esta rede social possibilita um meio onde vários indivíduos possam protestar e organizar-se contra o poder político, abrindo portas para a luta contra a opressão política ou certos regimes políticos.

Numa perspetiva geral, e apesar de vivermos nas sociedades com maior recurso a informação, este facto não é sinónimo de sermos a sociedade mais informada. A falta de critério e a elevada percentagem de informação disseminada sem que esteja certificada torna o processo de recolha de informação extremamente complexo e impreciso. Com efeito, as notícias publicadas nos OCS tradicionais estão normalmente sujeitas a um código de conduta, implicando a verificação, o exercício do contraditório e a apresentação de provas factuais que sustentem os conteúdos difundidos (seja em jornais digitais ou impressos, na televisão ou na rádio).

É precisamente devido aos desafios colocados na atualidade face à profusão de informações e de desinformação que deve ser feito um esforço para compreender de que modo é que podemos identificar estas ameaças previamente e, inclusive, definir estratégias que consigam dissuadir terceiros de produzir e partilhar desinformação.

1.3.3. Formas de deteção

Para Camargo e Bradshaw (2021), a evolução tecnológica que possibilitou a fácil circulação de desinformação ficou acentuada devido às inovações tecnológicas associadas ao desenvolvimento da Inteligência Artificial (IA). A IA permite a partilha automatizada de informações que através de algoritmos inseridos nas máquinas, “humanizam” a informação que é libertada para a esfera pública.

O próprio desenvolvimento tecnológico pode e deve ser usado no combate à desinformação, pelo que devem ser desenvolvidos meios ou técnicas que permitam a identificação precoce de fontes maliciosas de partilha de informação e mecanismos para as apagar, nomeadamente por parte das Polícias, no âmbito da prevenção e combate ao terrorismo, radicalização, recrutamento e campanhas de desinformação que promovam a apologia do ódio. A forma mais eficaz de prevenir *Fake News* passa pela identificação precoce destas mesmas notícias e por ser possível identificar as fontes e removê-las da *Internet*. A EUROPOL através da *European Cyber Crime Center* (EC3), por exemplo, apoiou os Estados-Membros na investigação de redes de cibercriminalidade, mas também na deteção e remoção, a pedido dos Estados, de conteúdos maliciosos publicados na rede.

Aldwairi e Alwahedi (2018) desenvolveram uma proposta de utilização de um mecanismo cujo objetivo específico passa por detetar e eliminar páginas da *Internet* que contenham informações erradas com o propósito de enganar e ludibriar os leitores. Este mecanismo consiste em fazer a transferência e a instalação de uma ferramenta para um computador que entra em ação assim que o utilizador inicia a pesquisa nos navegadores da *Internet* e

> Ao fazê-lo, a extensão identificará sítios cujas ligações contêm palavras que podem ter um efeito enganador para o leitor. Tais páginas web serão assinaladas como potenciais fontes de notícias falsas, e o utilizador será notificado antes de optar por aceder a qualquer uma delas. (Aldwairi & Alwahedi, 2018, p. 218).

Para Shu et al. (2020), a identificação precoce de informações falsas é a forma mais eficaz de reagir perante as *Fake News*. Uma outra forma de identificação destas informações passa pelo *vetting check* das mesmas. Maro et al. (2018) defendem que, embora este seja um método mais entediante e que pode não conseguir alcançar o objetivo pretendido, a sua aplicabilidade não deixa de ser pertinente.

Maro et al. (2018) estabelecem algumas hipóteses relativas ao processo *de vetting check*. Estes autores consideram que o processo de verificação das ligações pode ser melhorado se as ferramentas informáticas fornecerem informações úteis para os analistas humanos. Apesar

de termos máquinas e programas cada vez mais desenvolvidos, estas não possuem a sensibilidade na análise de certas informações sensacionalistas ou falaciosas, pelo que as máquinas não podem substituir os Homens a cem por cento.

A opinião dos autores fundamenta-se na oferta de informação contextual que, juntamente com as próprias informações, permite aos analistas humanos adquirir a capacidade de tomar decisões mais fundamentadas com base na verdade.

Como pudemos constatar, embora tenha sido verificada uma aceleração exponencial na revolução tecnológica, as máquinas ainda não conseguem substituir os Homens por inteiro. O apoio destas ferramentas tecnológicas é fundamental na desconstrução de (des)informação *online*, e como tal, devem ser implementadas estas ferramentas no seio policial. Precisamos de perceber e estudar os mecanismos utilizados pela Polícia de Segurança Pública em matéria de produção de inteligência, de modo a mitigar a utilização de eventuais informações enganosas nas fases de preparação e planeamento de operações e eventos de grande envergadura.

Capítulo II- Ciclo de Produção de Inteligência

2.1- Conceptualização

2.1.1- Enquadramento

A Constituição da República Portuguesa (CRP) é clara na definição das funções da PSP. O artigo 272.º da *lex matter* atribui à PSP as funções de garantia da defesa e da legalidade democrática, a garantia da segurança interna e os direitos e liberdades dos cidadãos. Por sua vez, a Lei de Segurança Interna, Lei n.º 53/2008, de 29 de agosto, doravante LSI, define no art.º 1.º que a segurança interna é a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática.

Elias (2018) define que a atividade de Polícia está estruturada através de cinco pilares: a Prevenção Criminal, a Investigação Criminal, a Ordem Pública, a Inteligência Policial e a Cooperação Internacional. Relembrando um princípio clássico do Direito Penal, Beccaria (2007) defendia que mais valia prevenir os delitos que os punir, atribuindo de igual forma um valor acrescido na prevenção da criminalidade.

Entendemos que o papel da Prevenção Criminal assume uma grande relevância na garantia da missão de polícia, "sendo a função primordial da polícia em qualquer estado de direito democrático" (Elias, 2017, p. 89), no sentido em que ajuda a evitar, ou minimizar possíveis consequências. Devem ser adotadas estratégias e privilegiar métodos de intervenção que contribuam no seu todo para reforçar a prevenção criminal.

A disseminação de *Fake News* pode induzir e impulsionar um conjunto de atitudes e comportamentos que, por sua vez, podem ter impactos negativos na vida em sociedade. Neste âmbito, e decorrente das atribuições legalmente atribuídas, compete à PSP a monotorização e controlo permanente de eventuais ameaças que possam surgir e que possam por em risco a segurança, ordem e tranquilidade públicas. Contudo, a facilidade de acesso e difusão de

qualquer tipo de informação dificulta o trabalho de monotorização pelo que, anualmente, são definidas um conjunto de Áreas de Interesse Permanente (AIP), em conformidade com a Norma de Execução Permanente (NEP) N.º AUOOS/DIP/02/05 de 30 de dezembro de 2014.

As AIP são as áreas de atividade de inteligência policial, definidas ao nível estratégico, e sobre as quais recaem os deveres de iniciativa e exploração sistemática de todas as fontes de informação disponíveis, por parte de toda a estrutura orgânica e efetiva do Sistema de Inteligência Policial (SINTEL) da PSP. Estas áreas são definidas de acordo as estratégias adotadas pela PSP, com o intuito de prevenir eventuais ameaças que possam por em causa a tranquilidade e ordem pública e a garantia da segurança interna.

Também no âmbito da atividade policial, a PSP definiu a nível estratégico, através da NEP n.º AUOOS/DO/01/24 de setembro de 2016 referente aos níveis de comando e controlo da PSP, diferentes tipologias de operações, nomeadamente: operações de rotina; operações inopinadas; e operações planeadas. De entre estas, e tendo em consideração o objetivo do presente estudo, optamos por abordar o caso concreto das operações planeadas, uma vez que exigem um maior esforço de planeamento prévio, nomeadamente no que concerne ao tratamento de fontes de informação e produção de inteligência.

2.1.2- Definição de Inteligência

Para Fernandes (2014, p. 79), o conceito de inteligência transcende a mera discussão e construção teórica pelas implicações políticas e para a política. A construção de um conceito unânime de inteligência é impraticável, uma vez que a doutrina não reúne consenso na sua caracterização.

De acordo com a Infopédia (2022, s.p.), o conceito de Inteligência pode abarcar várias definições, nomeadamente "(1) conjunto de todas as funções mentais que têm por objeto o conhecimento; (2) a faculdade de compreender; (3) conhecimento conceptual e racional; intelecto; (7) juízo; raciocínio; (14) entidades ou conjunto de pessoas que se dedicam à recolha de informações relativas à segurança de um estado.".

Khan (2009, como citado em. Fernandes, 2014) define, de forma simplista, inteligência como informação. Como tal, a informação deve ser devidamente tratada e analisada, de modo a garantir sustentação à decisão do decisor policial, na sua atividade.

Segundo Gill e Phythian (2018), o ponto de partida para definir inteligência é reconhecer que a inteligência é um meio para atingir um fim, sendo que o fim visado é, primordialmente, o de garantir a segurança. Através da garantia da segurança, a entidade que recolhe e utiliza a inteligência consegue prosperar e adaptar-se a qualquer realidade e/ou problema.

Breakspear (2012) propõe uma nova definição de inteligência. Para este autor, a inteligência é uma capacidade que possibilita a previsão da mudança a tempo de fazer algo sobre isso. Esta capacidade envolve previsão e perspicácia, e "destina-se a identificar mudanças iminentes, que podem ser positivas, representando oportunidade, ou negativas, representando uma ameaça" (p. 12).

Para Turner (2017), a inteligência pode ser definida através do conjunto de informação recolhida de várias fontes e tecnologias e que tem que ser posteriormente analisada. Fernandes (2014, p. 104) conclui que "a inteligência resulta do produto de um valor informacional acrescentado resultante de um processo específico, desenvolvido num conjunto de atores (…) que visa responder a necessidades específicas dos decisores".

O fundamento da inteligência passa pela necessidade de garantir o suporte necessário para a tomada de decisão aos diversos níveis: nível tático, operacional e estratégico. Omand (2010, p. 22.) reforça "que o objetivo mais básico da inteligência é melhorar a qualidade da tomada de decisões, reduzindo a ignorância.".

No âmbito da sua aplicação, podemos distinguir vários tipos de inteligência, consoante a sua finalidade. A NEP n.º AUOOS/DIP/02/05 de 30 de dezembro de 2014 estabelece que a inteligência policial compreende as estruturas e atividades cujo objetivo passa pela produção e difusão de inteligência relativa aos riscos que impedem sobre as missões e as atividades policiais, visando contribuir para a redução da surpresa e da incerteza inerentes à tomada de decisão, e para a eficácia, eficiência, a proatividade e a resiliência da PSP. A NEP suprarreferida

distingue ainda dois tipos de inteligência policial: a estratégica, ao nível da Direção Nacional (DN), e a operacional, ao nível das Unidades Policiais.

Para Fernandes (2014, p. 165) a inteligência policial como atividade

> é caracterizada como a aplicação de um conjunto de metodologias e técnicas especificas a dados e a informações de natureza diversa (policiais e não policiais) com o objetivo de produzir inteligência que identifica e avalia os riscos que impedem sobre a sociedade e sobre as atividades policiais, contribuindo para a proatividade policial (pela redução da incerteza e da surpresa) e para a otimização da utilização de recursos. (Fernandes, 2014, p. 165)

2.2.- Ciclo de Produção de Inteligência

2.2.1 O Ciclo de Produção de Inteligência

A NEP n.º AUOOS/DIP/02/05 de 30 de dezembro de 2014 define o Ciclo de Produção de Inteligência (CPI) como o processo dinâmico, continuo e interativo que permite a transformação de informações, de origens e natureza diversas, em inteligência policial. Este é o processo que garante que a produção de inteligência satisfaça as necessidades institucionais.

Marrin (2009) define o CPI como um dispositivo heurístico utilizado para encaminhar o fluxo de informação para os órgãos responsáveis pela produção de inteligência e para os respetivos decisores. Este autor apresenta uma teoria descritiva em que a inteligência é o ponto de partida para a interação entre os factos, o conhecimento e a posterior tomada de decisão.

Para Fernandes (2014, p. 105), a produção de inteligência "é tradicionalmente representada como um processo cíclico no qual os dados e as informações são transformados em inteligência.". De modo a perceber o processo de transformação de informação em inteligência, importa distinguir o conceito de inteligência do conceito de dados e de informação.

Os dados são o ponto de partida do processo de construção de inteligência. Estes são o conjunto de atributos diretamente observáveis na sua forma mais simplista, isto é, sem que haja recurso a qualquer tipo de tratamento. Por sua vez, a informação trata-se do conjunto de dados que quando analisados e contextualizados possuem um valor informacional a partir do qual poderá ser produzida a inteligência.

Fernandes (2014) e Omand (2010) apresentam-nos um ciclo tradicional de produção de inteligência que apresenta cinco fases (ver Anexo 1). O dinamismo deste processo permite que o ciclo se inicie em qualquer uma das cinco fases, potenciando a sua aplicabilidade e aumentando a quantidade de inteligência que se pode produzir.

A fase de planeamento consiste na definição das necessidades de inteligência. Conforme referido, anualmente são definidas AIP pela DN da PSP. Estas áreas representam as maiores preocupações em matéria de segurança, pelo que a produção sistemática de inteligência referente a estas mesmas áreas é, de todo, pertinente para o promover a sua dissuasão e a facilitação da prevenção de certos ilícitos criminais.

Fernandes (2014) afirma que nesta fase é executada uma gestão a nível macro das restantes atividades do ciclo, explicitando de que modo é que as restantes fases do ciclo contribuem para dar resposta às necessidades impostas. Marrin (2009) defende que o início do CPI se dá através dos requisitos de informação de que os decisores necessitem.

Numa perspetiva policial, e à luz destes autores, entendemos que o CPI tem início pela necessidade de obtenção de informação sobre determinados assuntos, ou atores. Uma vez que o nosso trabalho tem como objeto de estudo as operações planeadas, importa perceber e determinar a importância que a produção de inteligência tem para garantir o sucesso destas operações.

Na construção de uma operação planeada, podemos identificar três fases cruciais onde o papel das informações e da inteligência policial se assume como essencial: a fase prévia à operação, durante a operação, e a fase posterior à operação, através da elaboração de relatórios de inteligência discriminados que possam vir a ser utilizados em operações futuras. Iremos de

igual modo abordar e aprofundar cada uma destas fases do planeamento, averiguando as principais fragilidades em cada uma delas.

As fases consequentes do CPI consistem na pesquisa e no processamento. Marrin (2009) refere que a maioria dos esforços para compreender o papel que a inteligência desempenha começa no ambiente externo. É através deste meio que são utilizados os vários instrumentos de recolha de dados para adquirir informações e proceder ao posterior processamento dos dados.

Nesta segunda fase de processamento os dados, as informações são avaliadas consoante o seu valor, fazendo-se assim uma primeira triagem. Nesta fase do processo, estes dados são indexados e dispostos para serem posteriormente analisados. Ainda, e de acordo com Gill e Phythian (2018), o processamento de informação pode ser uma fase problemática, uma vez que a informação depende sempre do contexto de onde é retirada. O processamento destes dados e informações exige um esforço acrescido no sentido de fazer a sua primeira interpretação, auxiliando assim a fase de análise da informação.

Johnson (2009, p. 41) defende que a "inteligência raramente vale por si própria". Este autor afirma que a inteligência deve ser interpretada com inteligência, isto é, através de pessoas altamente formadas e que consigam compreender e interpretar um conjunto diverso de informações. O esforço de pesquisa relativo a estas informações deve ser feito tendo por base o auxílio de meios tecnológicos que permitam a interpretação e a criação de correlações entre dados e informações.

Não obstante, Gill e Phythian (2018) afirmam que a transformação moderna das informações através de tecnologias sofisticadas nem sempre é a mais adequada, uma vez que, o processo de análise de informação continua a ser um processo intelectual. Conforme mencionado ao longo do nosso trabalho, apesar do exponencial aumento da tecnologia, as máquinas desenvolvidas ainda não conseguem fazer uma substituição total do Homem, uma vez que não conseguem substituir a capacidade de interpretação das emoções associadas às informações e aos contextos de onde estas são inseridas.

Ainda assim, Johnson (2009) faz referência ao termo de valor acrescentado. Para este autor, e em conformidade com Gill e Phythian (2018), o Homem possui e atribui um valor

acrescentado a todas as informações que por si são produzidas, uma vez que o analista consegue discernir das fontes de onde este recolhe a informação, podendo inclusive descartar fontes consoante a sua credibilidade.

Em consonância com estes autores, Fernandes (2014, p. 118) refere que os analistas não se limitam a "reorganizar e apresentar as informações num novo formato, mas que têm a função de determinar a relevância das informações disponíveis e produzir inferências com base nas mesmas. "

Por último, a fase da difusão da informação "consiste no processo de distribuição de inteligência aos consumidores" (Lowenthal, 2008, como citado em Fernandes, 2014, p. 123). Esta difusão de informação obedece a um conjunto de princípios elencados na NEP N.º AUOOS/DIP/02/05 de 30 de dezembro de 2014, nomeadamente através do princípio da oportunidade e do princípio da necessidade de conhecer.

De acordo com a NEP suprarreferida, o princípio da oportunidade define que a difusão de informações ou inteligência deve ser tempestiva, de modo a que o seu destinatário a possa explorar e interpretar em tempo útil, enquanto que o princípio da necessidade de conhecer refere que todas as atividades desenvolvidas no âmbito do SINTEL estão sujeitas, em permanência, a medidas de segurança, garantido que informações e inteligência apenas são cedidas a quem está credenciado e tem efetiva necessidade de conhecer.

2.2.2 Fontes de Inteligência

A pertinência do estudo das fontes de inteligência passa pela diversidade de métodos que podem ser utilizados com o objetivo de recolher informações e dados. Uma vez que as *Fake News*, tendencialmente, têm maior expressão no meio digital, existe uma necessidade de perceber quais são as fontes disponíveis e de que modo se pode evitar a recolha de informações falaciosas.

Gill e Phythian (2018) apresentam-nos uma diversidade de fontes de informação (ver Anexo 2). Através do Anexo 2, conseguimos observar que existem sete formas principais de

obtenção de informação, que se podem subdividir noutras categorias: o OSINT (Open Sources Intelligence), a SOCMINT (Social Media Intelligence), a PROTINT (Protected Information Intelligence), a HUMINT (Human Intelligence), a SIGINT (Signals Intelligence) a IMINT (Imagery Intelligence) e a MASINT (Measurements and Signatures Intelligence).

A HUMINT representa o meio mais tradicional de obtenção de inteligência (Gill & Phythian, 2018, p. 130). Esta consiste na inteligência que é

> produzida através das atividades de pesquisa em que os seres humanos usam como principal meio de pesquisa os seus sentidos (…) e inclui todos os tipos de dados e informações recolhidas pelos seres humanos a partir de fontes abertas ou classificadas, pelo recurso à observação direta de comportamentos, eventos ou objetos. (Fernandes, 2014, p. 111)

O OSINT é um tipo de inteligência que é processado e analisado a partir de informação publicamente disponível de fontes abertas e de documentos não classificados (Ivanjko, 2019). Por se tratar de um conjunto tão amplo de fontes de dados, é de todo pertinente que existam canais técnicos próprios, de modo a canalizar e categorizar o tipo de informação recolhida.

O facto de vivermos em sociedades cada vez mais digitalizadas, abre-se portas a que sejam exploradas novas ferramentas para obter informações. Para Omand et al. (2012, p.804) a SOCMINT surge no sentido de compreender "a visão dos milhares de utilizadores das redes sociais e perceber as relações que estes criam". Estes autores afirmam que conhecer e dominar o conteúdo das redes sociais permite aos organismos públicos compreender e responderem aos inputs externos, e prever eventuais problemas que possam surgir.

De acordo com Omand (2010), a PROTINT é a informação pessoal e individual dos cidadãos que está guardada em bases de dados de ambos os setores, público e privado. Estes dados estão muitas vezes relacionados com dados de identificação civil e com as preferências comerciais e respetivos hábitos de compras das pessoas. Estas informações são guardadas pelas bases de dados através das designadas cookies, que, quando aceites, transformam e influenciam as escolhas dos utilizadores consoante as suas tendências.

Elias (2019) afirma que o desenvolvimento tecnológico "criou uma ilusão no seio da comunidade de inteligência (policial e nos serviços de informações), de aposta e de confiança na inteligência técnica. Fernandes (2014) reforça esta ideia e refere uma nova categoria de fonte de inteligência: a TECHINT (Techincal Intelligence), que considera ser "uma forma cada vez mais importante de inteligência" (Fernandes, 2014, p. 111). Esta nova categoria vem agrupar e consolidar um conjunto de outas fontes como o SIGINT, o IMINT e o MASINT.

Gill e Phythian, (2018) definem IMINT como a informação derivada das fotografias e das imagens eletrónicas, incluindo as imagens retiradas de satélites. A MASINT é a "inteligência que resulta da análise científica e técnica de dados e informações obtidos por sensores específicos com o objetivo de identificar as características dos seus emissores" (Fernandes, 2014, p. 113).

Por último, Gill e Phythian, (2018) definem SIGINT como a informação que deriva da interceção de comunicações e outros sinais eletrónicos. A diversidade de meios e de sinais que podem ser intercetados exigiu a criação de subcategorias de modo a controlar todos estes sinais, dividindo-se em COMINT (Communications Intelligence), em ELINT (Eletronic Intelligence) e em FISINT (Foreing Instrumentation Signals.).

Elias (2019) refere que a elevada aposta na obtenção de Inteligência através dos recursos tecnológicos gerou uma desvalorização gradual dos meios mais tradicionais como a HUMINT. Não obstante, todos estes meios de obtenção de inteligência devem ser operacionalizados em consonância, de modo a conseguir obter sempre o melhor produto de inteligência possível. A maior e melhor disponibilidade de informação permite aos decisores policiais a tomada de decisões mais adequadas e fundamentadas, oferecendo melhores respostas aos problemas que se colocam.

2.3- A Inteligência nas Operações Policiais

2.3.1- As Operações planeadas

2.3.1.1- A fase de preparação. De acordo com a Infopédia (2022, s.p.), o planeamento consiste no "1. ato ou efeito de planear; 2. determinação de objetivos e dos meios para os atingir; 3. preparação de decisões para alcançar objetivos específicos tendo como finalidade melhorar o uso e a gestão dos recursos bem como a qualidade dos ambientes naturais e sociais; 4. função ou serviço de preparação do trabalho".

Neste sentido, existe um conjunto de preocupações que devem ser tidas em conta aquando a preparação de uma operação policial. Assim que seja dado o conhecimento de que irá decorrer um evento, devem ser tomadas de imediato medidas com o intuito de dar início a um conjunto de ações para garantir o sucesso do mesmo.

Com o planeamento de um grande evento, pretende-se atingir múltiplos objetivos: desde logo adequar os recursos às várias atividades conhecidas; identificar possíveis cenários que possam ocorrer tendo em consideração toda a informação disponível; e procurar antecipar riscos e ameaças de forma a identificar formas de os eliminar ou mitigar o seu impacto no evento. Para atingir estes objetivos, a atividade de recolha e tratamento de informação assume um papel determinante em toda a fase de planeamento.

No âmbito das suas atribuições, o Sistema de Inteligência (SINTEL) da PSP garante a recolha e análise das necessidades operacionais de inteligência, executando o CPI. Este primeiro esforço de pesquisa tem como objetivo recolher o máximo de informações possíveis para que seja possível traçar cenários e prever eventuais riscos para a segurança do planeamento.

A gestão das informações e a monotorização de eventuais *fake news* é crucial para a garantia do sucesso da missão. Conforme exposto, a disseminação deste tipo de notícias falaciosas é uma prática recorrente, pelo que devem ser adotadas medidas que garantam a fiabilidade das informações e das fontes das mesmas.

O *vetting check* e o cruzamento das informações, ainda que não garantam uma total fiabilidade das informações, possibilita aumentar a credibilidade das mesmas, adotando medidas mais adequadas aos planeamentos.

2.3.1.2- Durante o planeamento. No decurso do planeamento, a recolha e análise de informações em tempo útil permite a rápida reação e resposta a eventuais problemas que possam surgir e colocar em causa a segurança e o normal decorrer do policiamento. A versatilidade e a capacidade de adaptação dos recursos e dos meios são de todo cruciais para dar resposta às dificuldades que vão surgindo, de modo a garantir a missão da PSP, na medida em que o ambiente e as operações policiais são muito mais caraterizadas pela incerteza, imprevisibilidade e volatilidade do que as operações militares tradicionais.

Contudo e caso sejam detetadas eventuais *fake news*, nesta fase, a sua verificação e validação torna-se uma tarefa extremamente difícil e muitas vezes impossível pela incapacidade de verificar em tempo útil a veracidade destas informações. Ainda assim, os decisores policiais devem ter em conta todas as informações recolhidas e traçar planos e cenários para a eventualidade de alguma destas informações/ameaças se concretizar.

A gestão dos meios e de recursos é dificultada pela difusão de *fake news*, uma vez que há uma necessidade de adaptação constante à realidade e de dar reposta a eventuais ameaças que podem nem sequer vir a concretizar-se, despendendo-se meios para o efeito, e muitas vezes desviando recursos de locais que podem criar fragilidades em termos securitários. Neste caso a afetação/desvio dos recursos deve ser sempre ponderada, tendo em consideração o impacto que os riscos e ameaças de cada cenário pode criar para o desenrolar do evento.

Os decisores policiais devem ter em conta as eventuais informações que possam surgir antes, durante e depois das operações e, sempre que possível, tomar medidas, ou preparar ações preventivas para o caso de se virem a concretizar estas eventuais ameaças. Conforme referimos, o ambiente em que a PSP se insere e as suas missões e operações podem ser influenciados por fatores estruturais (mais previsíveis), mas também por questões conjunturais (normalmente inesperadas), mais difíceis de antecipar.

Um exemplo sintomático do recurso a desinformação por parte de grupos extremistas e inorgânicos consistiu nas publicações nas redes sociais durante os anos de 2011 e 2012, período muito marcado pela contestação social contra a carestia e desemprego resultante da intervenção da Troika em Portugal. Nessa fase, surgiram diversos *posts* na rede, os quais acabaram por ser divulgados pelos órgãos de comunicações social tradicionais, a acusar a PSP

de se infiltrar nas manifestações públicas de protesto com polícias à civil, com vista a provocar desacatos e assim justificar intervenções musculadas e detenções.

Essas publicações e notícias divulgaram fotos de alguns polícias da investigação criminal da PSP a intercetar manifestantes nessas ações de contestação contra as políticas do Governo. Todavia, estas intervenções eram realizadas após a verificação de atos violentos entre manifestantes, contra os polícias ou para quebrar perímetros de segurança (por exemplo, em frente à Assembleia da República). Alguns destes grupos transmitiam imagens em direto (*streaming*) na internet e procuravam manipular a audiência com relatos conspirativos e falaciosos. Estas *Fake News* acabaram por ter alguma visibilidade nas redes sociais, na televisão e imprensa e, embora não tendo qualquer sustentação, tiveram um impacto negativo na imagem institucional da PSP. Por isso, em face destes exemplos, as Forças e Serviços de Segurança deverão definir estratégias de comunicação mais proativas, no sentido de desmontar narrativas fictícias que procuram deslegitimar a ação dos polícias.

Por isso, avaliação do risco deve ser constantemente atualizada, de modo a garantir que as decisões tomadas são as mais corretas, sempre de acordo com a fundamentação que é obtida pelos relatórios de inteligência, em conjugação com as informações obtidas em tempo real. Nesse sentido, será crucial que a PSP incorpore, na fase de planeamento de eventos de grande envergadura, o policiamento da rede e uma análise sistemática de fóruns e grupos de conversação previamente identificados, de forma a detetar eventuais fontes de ameaça (grupos extremistas, terroristas, grupos organizados de adeptos, grupos criminosos, movimentos de cidadãos, etc.), cujas intenções possam colocar em causa a segurança do evento e das operações policiais, bem como violar direitos, liberdades e garantias. Serão relevantes, naturalmente, o planeamento de desordens públicas ou de ações contra as Forças de Segurança, no âmbito de reuniões ou de manifestações, o planeamento de atentados terroristas, a preparação de confrontos entre grupos organizados de adeptos, a convocação de manifestações espontâneas que impliquem com os direitos de terceiros (cortes de estrada, ocupação de espaço público ou privado, etc.).

Dependendo da dimensão e importância do evento, o número de recursos a empenhar pela PSP pode ser maior (quer ao nível do Departamento de Informações Policiais - DIP, quer

ao nível do Comando Metropolitano/Regional ou Distrital), podendo ainda contar com o apoio de outras Forças e Serviços de Segurança.

2.3.1.3- A fase de execução. Durante a operação de segurança de um grande evento, será fundamental a instalação de postos de comando estratégico, de postos de comando operacional e de postos de comando tático, conforme doutrina em vigor na PSP, justificando-se estes três níveis de comando e controlo apenas nas operações nacionais e/ou de elevada complexidade, em conformidade com a NEP n.º AUOOS/DO/01/24 de setembro de 2016. Nas operações mais críticas e complexas (por exemplo, levada a efeito na operação de segurança do EURO 2004, da Cimeira da NATO em 2010 ou da Liga das Nações em 2018), constitui uma boa prática a instalação de uma célula de informações junto ao Posto de Comando Operacional, no sentido, entre outras missões, de analisar em permanência as redes sociais, em particular fóruns previamente identificados ou chats de grupos extremistas que se configurem como fontes de ameaça destas operações. Aquando da operação de segurança da Cimeira da NATO em novembro de 2010 – evento em que participaram sessenta chefes de Estado e de Governo -, a célula de informações instalada junto do Posto de Comando Operacional foi integrada por analistas da PSP, PJ e SIS, facto que constituiu uma verdadeira inovação e foi fator crítico de sucesso para identificar ameaças e riscos à segurança e ordem públicas.

2.3.1.4- A fase posterior. A última fase do planeamento consiste na realização de *debriefings*. Através da realização de *debriefings* é possível analisar todo o percurso do planeamento, a execução do policiamento e identificar os pontos fortes e fragilidades. Ao realizar esta atividade é possível identificar as falhas e encontrar as possíveis soluções para as mesmas, e a documentação desta análise permite que, em eventos futuros, mesmos com atores e decisores policiais diferentes seja possível realizar um planeamento mais completo, colmatando as falhas e fragilidades previamente identificadas.

Nesta fase, não existe um impacto direto despoletado pela disseminação das *Fake News*, uma vez que consiste exclusivamente na análise do planeamento do evento e na deteção

e recolha das informações que resultam do mesmo, documentar e analisar as lições aprendidas e as boas práticas de forma a serem replicadas em futuras operações.

À posteriori, devem ser analisadas todas as informações que foram recolhidas durante o policiamento e detetar as suas fontes. Perceber a origem destas fontes e a veracidade das suas informações é de todo crucial para suportar a decisão em eventos futuros, com base em informações que surjam durante os eventos, provenientes destes tipos de fontes. Será também crucial aprimorar procedimentos para que seja garantida a deteção precoce de ações de desinformação que visem promover a desordem pública ou outras ações subversivas que coloquem em causa direitos, liberdades e garantias.

A produção de inteligência deve ocorrer em todas as fases do planeamento de policiamentos e de todo o tipo de eventos. A existência da maior disponibilidade de informações para a tomada de decisão é fundamental para garantir que são tomadas as melhores decisões possíveis, tendo por base a informação recolhida e analisada.

Capítulo III - Método

Exposta a componente teórica da nossa investigação, surge a necessidade de perceber qual o caminho a traçar de modo a obter a melhor resposta para o nosso problema de investigação. Marconi e Lakatos (2017) explicam que o método consiste no conjunto das atividades racionais que nos permitem alcançar um objetivo, para que lhe seja garantido o devido rigor científico.

Na componente teórica da nossa dissertação, foi feito recurso à literatura existente de modo a "documentar a fonte das nossas ideias e para enriquecer a justificação que sustenta a questão de investigação" (Fortin, 2009, p. 68). Assim, o desenvolvimento do nosso estudo passou por, numa primeira fase, elaborar uma revisão de literatura, de modo a conhecer e expor "o estado-de-arte da investigação" (Sarmento, 2013, p.13) existente relativo às Ameaças Híbridas e ao Ciclo de Produção de Inteligência, limitando assim o objeto do nosso estudo.

A abordagem utilizada na nossa investigação, e tendo em conta a nossa problemática de investigação, foi a qualitativa, uma vez que este procedimento permite uma "compreensão absoluta e ampla do fenómeno em estudo" (Fortin, 2009, p. 22). De acordo com Marconi e Lakatos (2017, p. 224.), as entrevistas são consideradas por muitos autores como o "instrumento utilizado por excelência da investigação social".

Recorremos à utilização de entrevistas semiestruturadas, que de acordo com Campenhoudt et al. (2017, p. 262) "são certamente as mais utilizadas nas investigações.". A escolha deste tipo de entrevista prendeu-se com o facto de se obter o máximo de informação dos nossos entrevistados, com vista a alcançar um maior número de perspetivas, de pessoas que sejam consideradas pertinentes e especialistas em matéria das informações (Sarmento, 2013).

Assim, a nossa dissertação partiu do problema:

- Qual o impacto das *Fake News* na segurança e na ordem pública?

3.1-Corpus

Para Bardin (2016) o *corpus* consiste no conjunto dos documentos que são interpretados e posteriormente submetidos a processos de análise. Através destes documentos é-nos permitido analisar toda a informação versada e retirar e apresentar conclusões.

Assim o corpus do nosso estudo é composto por cinco entrevistas que foram transcritas e posteriormente analisadas.

3.2-Participantes:

No nosso estudo foi solicitada a realização de seis entrevistas. Contudo, e uma vez que um dos entrevistados não acedeu ao nosso pedido, apenas foram entrevistados cinco participantes. Dois destes são oficiais do COMETLIS e os restantes três estão diretamente relacionados com a área de produção de informação.

Os oficiais do COMETLIS entrevistados foram o Superintendente Domingues Urbano Antunes (licenciado em Ciências Policiais pelo Instituto Superior de Ciências Policiais e Segurança Interna, licenciado em direito pela Faculdade de Direito da Universidade de Lisboa, pós-graduado em direito e segurança com o grau de auditor de Segurança Interna pela Faculdade de Direito da Universidade Nova de Lisboa e pós-graduado em procedimento contraordenacional pelo Instituto Superior de Ciências Policiais e Segurança Interna. Do percurso profissional destacamos as passagens pelas esquadras de Cascais e Parede, Chefe da área operacional da divisão de Cascais, Diretor da Unidade Nacional de Informações e Investigação Criminal da ASAE, Inspetor na Inspeção Nacional da PSP, desempenhado atualmente funções de Chefe da Área Operacional do Comando Metropolitano de Lisboa), e o Intendente Francisco Alves, licenciado em Ciências Policias pelo Instituto Superior de Ciências Policiais e Segurança Interna, que concluiu o 34º Curso de Ordem Pública no ano de 2004 e concluiu o 1º curso de Comando e Direção Policial nos anos de 2014/2015. Do seu percurso profissional, destacam-se as passagens pela esquadra da PSP do aeroporto de Faro, esquadra de Olhão, Corpo de Intervenção de 2004 a 2015, adjunto de comandante das Divisões de Loures e de Cascais, estando de momento nas funções de Comandante da 3ª Divisão do COMETLIS. A

escolha destes oficiais é resultante das atividades profissionais que estes desempenham, uma vez que as suas funções passam pela gestão e comando de um grande conjunto de operações, que requerem um grande esforço de pesquisa para a realização do seu planeamento e execução do policiamento

Os restantes convidados foram a jornalista Tânia Laranjo (licenciada em Ciências da Comunicação pela Universidade Autónoma de Lisboa, que iniciou o percurso profissional em 1995 no Jornal de Notícias. Foi Grande Repórter do Público entre 2005 e 2007, e desempenha funções no Correio da Manha desde 2007, fazendo parte da sua fundação), o jornalista João Fernando Ramos (detentor de uma pós-graduação em direito da comunicação pela Universidade de Coimbra, com passagens pela Rádio Nova, Público, RTP e que atualmente desempenha funções na CNN), e o Professor Doutor. Fernando Zamith (licenciado em comunicação social e mestre em ciências da comunicação pela Universidade do Minho, doutorado em informações e comunicação em plataformas digitais pela Universidade do Porto). Este último foi também jornalista da agência Lusa entre 1988 e 2011, e é docente na Universidade do Porto desde 2002. Com a escolha destes convidados procuramos recolher a opinião de personalidades de reconhecidos méritos profissionais e académicos, que desenvolvem a sua atividade com base na recolha e divulgação de informações, e uma longa experiência e visão idónea e credível, e que pela natureza das suas funções lidam recorrentemente com o fenómeno das *Fake News*.

3.3 Instrumentos de análise

3.3.1- A entrevista

O instrumento de recolha de dados que optamos por utilizar na nossa dissertação foram as entrevistas. A escolha deste instrumento prendeu-se em grande parte com a possibilidade de, de acordo com Campenhoudt et al. (2017, p. 262), se retirar das entrevistas informações e elementos de "reflexão que são muito ricos e matizados" e "por produzirem uma riqueza de dados, recheada de palavras que revelam as perspetivas dos respondentes" (Bogdan & Biklen, 1994, p. 136).

Deste instrumento, podemos ainda retirar um conjunto de vantagens e mais-valias. Para Marconi e Lakatos (2017, p. 224), as entrevistas permitem que sejam "recolhidos dados e informações que não se encontram em fontes documentais, mas que são igualmente relevantes e significativos" para a investigação. A escolha de pessoas experientes na área da nossa investigação permite-nos recolher e beber da sabedoria deles e das suas experiências, aumentando o número de dados recolhidos que serão posteriormente analisados e tratados.

Bogdan e Biklen, (1994, p. 135) afirmam que as entrevistas "variam quanto ao grau de estruturação". Quanto à sua estruturação, as entrevistas podem assumir três tipologias. Wilson e Wincup (2004, como citado em Silverman, 2009, p. 108) caracterizam as" entrevistas como estruturadas, semiestruturadas e abertas". As primeiras caracterizam-se por serem entrevistas mais neutras e com ausência de improviso e estímulos para os entrevistados. As entrevistas abertas caracterizam-se por serem mais flexíveis para os entrevistados, não havendo um rumo predefinido para a entrevista. Por fim as semiestruturadas, utilizadas na nossa dissertação, caracterizam-se por permitirem, de acordo com Bogdan e Biklen, (1994, p. 135), uma maior recolha de dados que poderão ser posteriormente comparáveis entre si.

A utilização de entrevistas semiestruturadas permite-nos orientar os entrevistados por um guião que seja predefinido, podendo-se ainda esclarecer em qualquer momento da entrevista qualquer informação que não tenha sido percetível. Ainda, o facto de entrevistarmos pessoas experientes na área do nosso estudo, permite-nos obter um conjunto alargado de informações pertinentes e de experiências, das quais resultam numa análise mais rica e estruturada das entrevistas.

3.3.2 Analise de Conteúdo

De modo a proceder à análise do *corpus* da nossa dissertação, recorremos à análise das entrevistas. Para Marconi e Lakatos (2017) a análise de conteúdo consiste no processo que permite a descrição sistemática, objetiva e quantitativa do conteúdo retirado da comunicação.

A análise de conteúdo consiste numa "metodologia de tratamento e análise de informações constantes de um documento" (Severino, 2017, p. 92). Este autor adianta que este

processo trata de "compreender criticamente o sentido manifesto das comunicações" (Severino, 2017, p. 92).

Berelson (s.d., como citado em Bardin, 2016, p. 42) define análise de conteúdo como "a técnica de investigação que através de uma descrição objetiva, sistemática e quantitativa do conteúdo do manifesto das comunicações tem por finalidade a interpretação destas mesmas comunicações"

A análise de conteúdo pode ser caracterizada como "um conjunto de instrumentos metodológicos cada vez mais subtis em constante aperfeiçoamento, que se aplicam a "discursos "(conteúdos e continentes) extremamente diversificados" (Ghigloine, s.d., como citado em Bardin, 2016, p. 7).

Para Silverman (2009, p. 149) a análise de conteúdo é um método que assenta no estabelecimento de um número de categorias e na posterior contagem do número de vezes que as unidades de registo incidem em cada categoria, ressalvando que há uma "exigência crucial de que as categorias sejam suficientemente precisas para capacitar diferentes codificadores e chegar aos mesmo resultados"

Capítulo IV - Procedimentos

Uma vez que procedemos à entrevista de dois grupos distintos de pessoas, optamos pela elaboração de dois guiões de entrevistas. Um primeiro composto por nove perguntas, que foi entregue aos dois oficiais da PSP (ver Apêndice B), e um segundo guião composto por onze perguntas, que foi entregue aos restantes entrevistados (ver Apêndice A). Esta escolha prendeu-se com a possibilidade de alcançar um maior número de informação e conhecimento por parte dos nossos entrevistados, focalizando algumas perguntas consoante a sua atividade profissional.

Ambos os guiões de entrevista possuem um conjunto de cinco perguntas idênticas, divergindo nas restantes. As entrevistas foram realizadas de forma a conter um breve enquadramento da nossa dissertação, bem como dos objetivos pretendidos com as mesmas. As questões foram numeradas de forma a facilitar a análise e transcrição das entrevistas.

Os entrevistados externos foram escolhidos tendo em consideração a sua atividade profissional no âmbito das informações. Por sua vez, os entrevistados policiais foram escolhidos pelas funções que desempenham e o elevado volume de operações decorrente do exercício das suas funções.

Após a validação do guião das entrevistas, pelos orientadores, foi o mesmo remetido à Direção de Ensino do ISCPSI com vista à solicitação de autorização para a realização das mesmas (ver Anexo 3). Obtido o despacho favorável, procedemos aos contactos para agendar a realização das entrevistas. As mesmas foram realizadas entre os meses de fevereiro e março, tendo sido dado preferência ao método de entrevista presencial.

O convite para a colaboração na nossa dissertação foi enviado via *e-mail*, individualmente para cada um dos entrevistados, tendo sido posteriormente agendada a marcação das entrevistas, consoante a disponibilidade de cada um. Neste primeiro contacto, já foi explicado de forma muito sumária o tema da nossa dissertação, bem como o motivo da escolha do participante.

Em virtude da situação pandémica atual, e por devido a um dos entrevistados à data da entrevista se encontrar infetado por Covid 19, procedeu-se à realização da mesma através do envio do guião por email. Ainda, e por impossibilidade outro entrevistado, recorreu-se à

plataforma *Zoom*, para realizar a respetiva entrevista. As restantes entrevistas ocorreram conforme planeado, tendo sido realizadas presencialmente. Aos entrevistados foi apresentado um Termo de Consentimento Informado (ver Apêndice C), garantido um princípio ético de transparência para com os mesmos.

Conforme mencionado, no início de cada entrevista foi feito um breve enquadramento teórico aos entrevistados, bem como foram explicados os objetivos da entrevista, clarificando eventuais dúvidas. Foi mencionado que os mesmos poderiam desistir da entrevista em qualquer momento, ou esclarecer eventuais dúvidas em qualquer momento da dissertação. Foi solicitado aos entrevistados a gravação da entrevista, para que fosse facilitada a posterior análise, ao que todos consentiram. Assim, foram transcritas as cinco entrevistas que consistem no *corpus* da nossa investigação, para posterior análise de conteúdo.

O processo de análise iniciou-se com a definição de um conjunto de categorias. Foram definidas cinco categorias de acordo com "determinadas questões e preocupações de investigação" (Bogdan & Biklen, 1994, p. 221): Fake News (Categoria A); Informações (Categoria B); Operações Policiais (Categoria C); Redes Sociais (Categoria D); e por último Órgãos de Comunicação Social (Categoria E). A definição destas categorias resultou da pertinência que alguns dos fatores estudados na componente teórica da nossa dissertação assumiram e, à medida que se foi desenrolando a análise das entrevistas, o surgimento de novos temas de teor relevante para a nossa dissertação.

Dento da Categoria A foram criadas quatro subcategorias (A.1 a A.4). Na Categoria B foram criadas 3 subcategorias nomeadas de B.1 a B.3. Na Categoria C foram criadas cinco subcategorias nomeadas de C.1 a C.5. Na Categoria D foram criadas quatro subcategorias e, por fim, na Categoria E foram criadas quatro subcategorias.

Relativamente à Categoria A, foram criadas as subcategorias: A.1- Desinformação, correspondente à disseminação de desinformação; A.2- Manipular a realidade, correspondente a informações que incidissem sobre a manipulação e deturpação da realidade; A.3- Destabilização, correspondente às informações utilizadas predominantemente com o propósito de destabilização social; A.4- Resposta, correspondente à resposta que se poderá dar as *Fake News* de uma perspetiva geral.

Na Categoria B, foram criadas as seguintes subcategorias: B.1- Controlo de informação, correspondente ao controlo e monotorização das informações de um modo geral; B.2- Partilha de Informação, correspondente à disponibilidade e partilha de informação; B.3- Informações Sensíveis, correspondente à partilha de informações sensíveis e comprometedoras para a sociedade.

Dentro da Categoria C, foram criadas as seguintes subcategorias: C.1- Gestão das informações Policiais, que diz respeito ao controlo de todas as informações que chegam às policias, bem como ao controlo das fontes de informação; C.2- Inteligência Policial, correspondente à análise das informações policiais; C.3- Cenarização, correspondente à cenarização de toda e qualquer informação obtida; C.4- Resposta Policial, relativa à resposta que deve ser dada institucionalmente no combate à desinformação e às *Fake News*.

Na Categoria D foram criadas as seguintes subcategorias: D.1- Viralização, referente à viralização de informações nas redes sociais; D.2- Perceção, correspondente à perceção que as pessoas têm das redes sociais e à dificuldade de discernimento relativamente à informação que está disponível naquelas plataformas; D.3 Confirmação, relativa à confirmação e verificação das informações que circulam nas redes sociais; D.4- Gestão das redes sociais, referente à regulamentação ou falta da mesma das redes sociais.

Por último, na categoria E, foram criadas as seguintes subcategorias: E.1- Gestão da informação, referente ao modo através do qual os Órgãos de Comunicação Social (OCS) priorizam a escolha da sua informação; E.2- verificação, referente ao trabalho dos OCS em matéria de verificação das informações; E.3- Reação, referente à resposta dos OCS face, às *Fake News*; E.4- Visualização, referente ao impacto e ao alcance que os OCS possuem na sociedade.

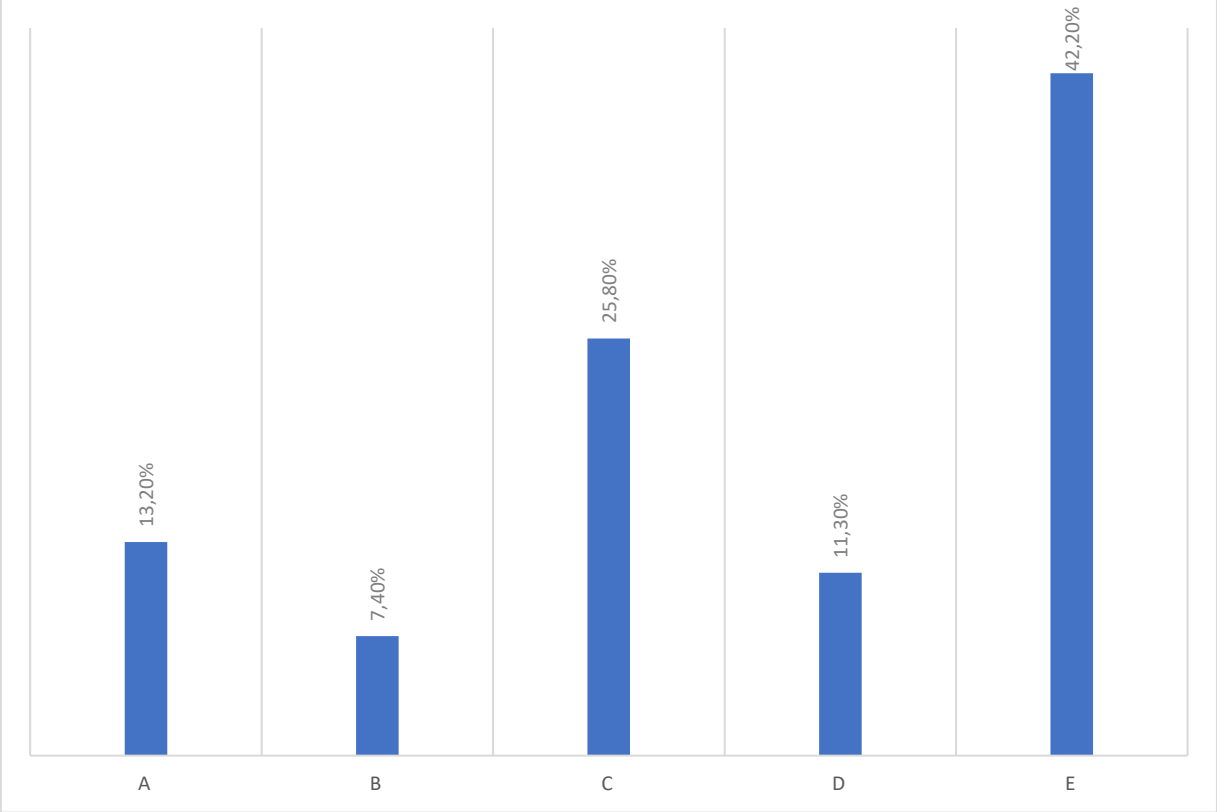
Finda a grelha categorial (Apêndice D), iniciamos o processo de codificação "de modo a organizar os dados" (Bogdan & Biklen, 1994, p. 221), assegurando para tal todos os critérios de validade, nomeadamente os princípios da exaustividade e da exclusividade. Procedemos assim ao tratamento e à interpretação dos resultados obtidos, e à contabilização das unidades de registo correspondentes a cada subcategoria, interpretando, *à posteriori*, os seus resultados.

Capítulo V - Apresentação e Discussão dos resultados

Neste capítulo da nossa dissertação estão expostos os resultados da análise do conteúdo. Iremos abordar as categorias consoante os números absolutos das unidades de registo (U.r) e a sua importância para o nosso problema de investigação, fazendo uma análise mais aprofundada das subcategorias de cada categoria. A figura que se junta é referente à distribuição percentual de cada categoria.

Figura 1

Distribuição percentual das categorias



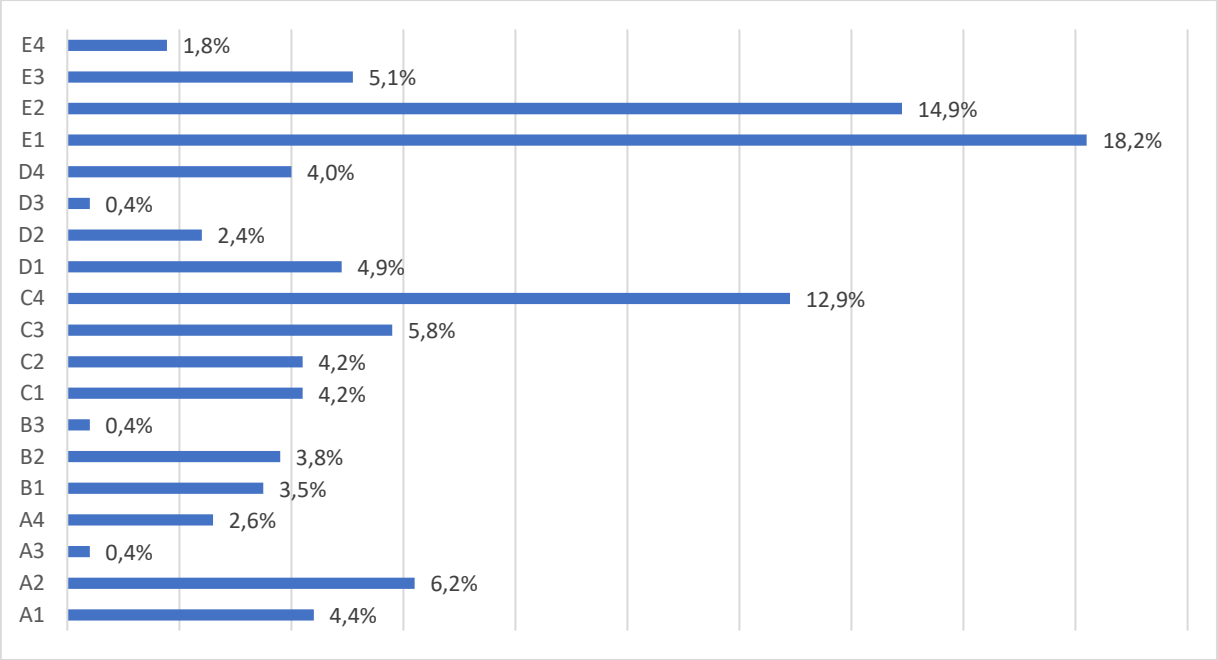
Nota. Elaboração própria com base na distribuição percentual das categorias

Conforme podemos constatar, as temáticas mais relevantes para os participantes concentraram-se no papel dos OCS (Categoria E), com 42,2% e na questão das Operações Policiais (Categoria C), com 25,8%. Com um menor destaque, mas igualmente pertinente para o cerne da nossa investigação, encontram-se a temática *Fake News* (categoria A), com 13,2% e a categoria relativa às Redes Sociais (Categoria D), com 11,3%. Os restantes dados encontram-

se inseridos na categoria das Informações (Categoria B), com 7,4% que corresponde a informações de caracter mais genérico.

Figura 2

Distribuição percentual das subcategorias

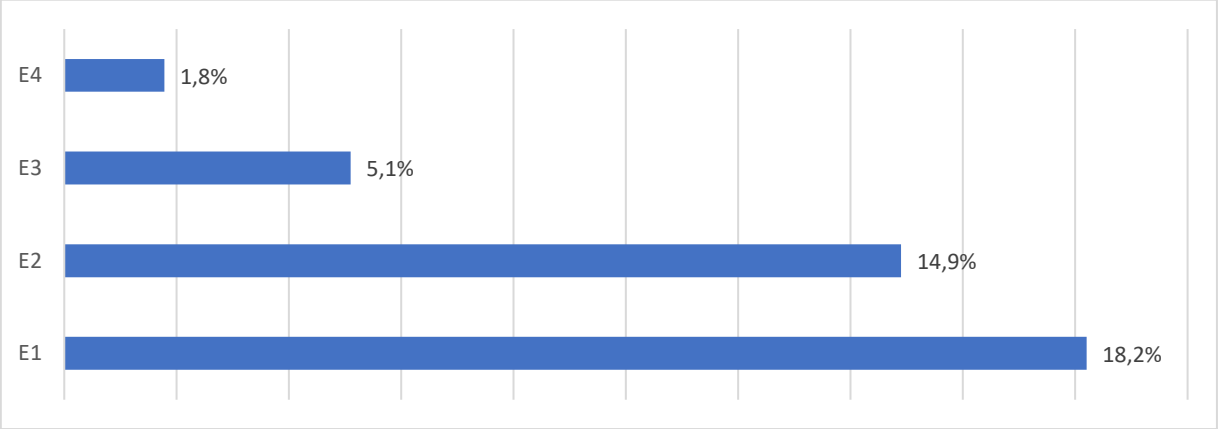


Nota. Elaboração própria com base na distribuição percentual das subcategorias

Com vista a analisar de forma mais aprofundada recorremos à figura que antecede, que apresenta a distribuição percentual de cada subcategoria. Deste modo, poderemos identificar as temáticas que os entrevistados consideraram mais relevantes para o estudo em apreço. Por outro lado, esta análise permite-nos compreender o impacto das *Fake News* na segurança e ordem pública, bem como as melhores formas de mitigar e minimizar esse mesmo impacto.

Figura 3

Distribuição percentual da subcategoria E



Nota. Elaboração própria com base na distribuição percentual da subcategoria E

Da análise podemos retirar que a variável a que os entrevistados atribuem maior relevância está relacionada com o papel dos OCS na Gestão da Informação (E.1, 18,2%), e o modo como a mesma é tratada. Para tal, devem os OCS corresponder a um conjunto de deveres éticos que deles se esperam. Conforme refere Antunes, "a comunicação social também deve corresponder a um ideal ético" e "a comunicação social tem o dever constitucional de informar o cidadão, por correspondência do direito do cidadão a ser informado.". Ainda neste sentido, identificamos a preocupação por parte dos OCS referente à necessidade de informar corretamente o cidadão. Nesta linha de pensamento Ramos refere que "nós temos a obrigação de informar o que é que está a acontecer", devendo para tal garantir a partilha de informação fidedigna respeitando os pressupostos éticos do jornalismo.

No que concerne à gestão da informação por parte dos OCS, também se nota uma preocupação com uma adaptação à realidade e à necessidade de se garantir um maior controlo das informações que circulam pelas redes sociais. Conforme refere Zamith, "grande parte da atualidade vive na internet, e muitos destes que vivem na internet, vivem nas bolhas das redes sociais, quase fechados, que não têm um mundo que não seja esse". Este afirma ainda que "os jornalistas têm sempre que medir o pulso à sociedade", existindo uma necessidade dos "Órgãos de Comunicação Social terem de estar presentes nas redes sociais", acrescenta Laranjo. Não obstante, Ramos refere que "podem ir ali buscar algumas notícias, mas não podem fazer a vida

em função das redes sociais" sendo que "não podemos correr o risco de estar a colocar no ar uma informação da qual não temos a certeza". "Nunca na vida. Isso não é jornalismo.", adita.

Não obstante, a elevada preocupação da gestão da informação, apuramos que a Verificação (E.2, 14,9%) da informação por parte dos OCS é de todo crucial para evitar a disseminação de eventuais *Fake News* e para garantir um fluxo de informação correta para todos os cidadãos, uma vez que estes possuem uma alta taxa de audiência, conforme podemos observar na subcategoria Visualização (E.4, 1,8%). No que diz respeito à comparação entre a disseminação da informação dos OCS e as redes sociais, Ramos esclarece que "temos que relativizar e perceber que são coisas completamente diferentes, não desvalorizar, mas relativizar". Este esclarece que embora existam "alguns vídeos virais que chegam a números assustadores, que podem atingir meio milhão/1 milhão de pessoas, dificilmente encontramos 10 milhões de visualizações num vídeo viral", enquanto que "uma notícia de televisão forte consegue praticamente chegar a todo o pais". Neste mesmo sentido, Zamith afirma que "ninguém gosta de ser enganado, pelo que a população vai voltar ao jornalismo credível das marcas que são de confiança e que existem no mercado, mas demora o seu tempo, infelizmente demora". Até ao aparecimento das redes sociais, "era mais fácil perceber o que era jornalismo e o que não era", destaca Zamith.

O desenvolvimento tecnológico e o aparecimento das redes sociais vieram exponenciar um novo campo aberto de diálogo e de partilha de informações e experiências para milhares de pessoas, e conforme constatado anteriormente, o jornalismo tem que acompanhar esta nova realidade, adaptando-se. Maior disponibilidade de informação não é sinónimo de maior disponibilidade de informação credível. Zamith refere que deve ser sempre adotada "a disciplina da verificação, que é uma das funções cruciais do jornalismo". Ramos acrescenta que "em circunstância alguma devemos amplificar uma informação da qual não temos a certeza que seja verdadeira", e finaliza afirmando que "nós temos que duvidar de tudo, faz parte do nosso ADN".

Por último, e ainda dentro do campo da Verificação, constata-se que é dado um especial enfoque ao trabalho que tem vindo a ser desenvolvido pelos OCS em matéria de verificação da informação, e o impacto que a atividade dos jornalistas têm na sociedade. Antunes refere que "não é por acaso que as cadeias de televisão têm vindo, em todos os canais, a produzir programas como o polígrafo. Muitas vezes, é o próprio jornalista que faz um exercício de investigação para

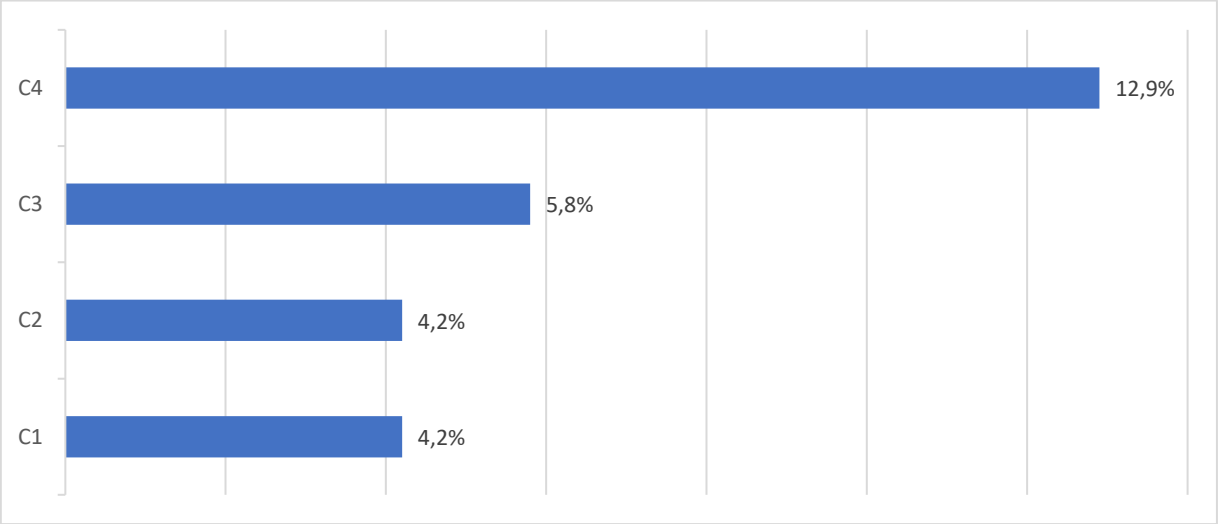
chegar à conclusão se aquilo é verdade ou mentira". Laranjo reforça esta ideia referindo que "cada vez mais tem que se criar mecanismos que ajudem o leitor a perceber que a informação é credível.", garantindo a consciencialização da população para o que é verdade ou não.

Relativamente à Resposta (E.3, 5.1%) que deve ser dada às *Fake News* pelos OCS, recolhemos algumas estratégias distintas. Ramos começa por referir que "se nós tivermos uma informação de uma rede social, se nós não a amplificarmos, se nós não lhe dermos crédito nos meios de comunicação convencionais, o tempo vai acabar por matar essa informação com a realidade", mas não deixa de parte a opção de as desmentir, uma vez que "às vezes não há espaço para esperar todo esse tempo, para que a realidade entre pelos olhos dentro de quem está com aquela informação falsa". Zamith concorda com esta posição e refere que "é um risco grande de alguns meios de comunicação. O jornal Público por exemplo, costuma ser bastante rigoroso com isso e se há alguma coisa que seja viral, mas que se saiba que é falso, o Público nem sequer faz notícia a denunciar e a dizer que aquilo é falso" para não correr no risco de aumentar a visualização daquela informação, mitigando, desta forma, o impacto que essa informação pudesse vir a ter. Acrescenta ainda que alguns programas como "o polígrafo da SIC está, de alguma forma, a chamar à atenção para algumas coisas que as pessoas não tenham visto na *internet* e se calhar até vão ver porque acham piada e vão partilhar sabendo que aquilo é mentira".

Não existem estratégias perfeitas para garantir que se impeça a propagação de eventuais informações falsas, independentemente do meio onde se propagam. Como podemos constatar, o simples facto de desmentir informações publicamente pode amplificar a sua ação e aumentar a sua disseminação em meios de comunicação não convencionais, como as redes sociais. Todavia, quando tratamos de informações que possam ser de tal forma impactantes para a sociedade, devem ser adotadas medidas, através dos programas de *Fake Checking* desenvolvidos pelos OCS. "Se é um jogo difícil de se fazer? É. Muito!" afirma Laranjo, mas "tem que se encontrar um equilíbrio", acrescenta Ramos.

Figura 4

Distribuição percentual da subcategoria C



Nota. Elaboração própria com base na distribuição percentual da subcategoria C

A segunda categoria que demonstra maior predominância é a C que diz respeito às Operações Policiais, havendo um maior número de U.r na subcategoria que diz respeito à Resposta Policial (C.4, 12,9%) às *Fake News*. À semelhança do que se verificou na resposta dos OCS, verificamos que a reação por parte da PSP deve variar consoante a situação. Alves refere que "acredita que há situações em que o senso comum pode responder", mas "aquelas mais impactantes na vida das pessoas, relacionadas com uma intervenção da polícia e, portanto, com a própria instituição, exigem uma resposta institucional.". Por sua vez, Antunes considera que, no que diz respeito à polícia "quando se verificam notícias falsas, deve ser imediatamente emitido um direito de resposta". Considerando "que a Polícia se encontra inserida numa sociedade moderna, deve aproveitar e através de um gabinete de comunicação desmistificar imediatamente uma *Fake New*".

Ainda dentro desta subcategoria, os entrevistados realçam o papel da estratégia de comunicação da PSP, dando especial enfoque a estratégia de comunicação interna e externa. Ramos destaca ainda a importância das "polícias terem que perceber qual é o impacto que estas *Fake News* podem ter, e que muitas vezes são danos colaterais". Este adianta ainda que estes danos colaterais podem assumir diversas formas, nomeadamente ao nível de alteração de ordem pública, onde inclusive "alguns movimentos aproveitam situações que estejam a acontecer para

se manifestarem e protestarem". "No caso das polícias, é um dilema que se coloca sempre. Reprimir pode ter o efeito contrário do que se deseja, pelo que é preciso ter algum cuidado", alerta Zamith. A resposta da polícia deve ser sempre o mais ponderada possível, e a mais assertiva, de modo a evitar eventuais danos e perigos para a segurança e para a ordem pública. "A estratégia comunicacional, o momento como o fazer, esse é o segredo. E isso nem sempre é fácil, mas agora que o têm de fazer, têm", conclui Alves.

A Cenarização (C.3, 5,8%) da informação também constitui também uma grande preocupação dos nossos entrevistados, uma vez que, em muitas situações, é impossível averiguar a veracidade das informações que circulam associadas a um determinado evento. Antunes "dá uma réstia de verdade a todo o tipo de informações e faz o seu planeamento a contar com um cenário para essa informação" e estabelece, assim, "um plano de resposta, uma vez que as polícias não podem ser completamente estanques, nem herméticas, aqui o que tem de se fazer é adotar um princípio de flexibilidade", sendo que "não podemos subvalorizar" qualquer tipo de informação que nos chegue.

A criação de cenários hipotéticos constitui uma das formas de garantirmos que não se coloca de parte qualquer tipo de informação, por mais tendenciosa que possa parecer. Quando não se consiga validar as informações, Alves refere que "o que pode acontecer, pode não alterar totalmente o planeamento, mas cria-se um cenário hipotético, e estabelece-se uma reação para esse mesmo cenário". Daqui decorre que em muitas situações "já estivemos preparados para determinados eventos que não vieram a ocorrer", afirma Antunes. Contudo o mesmo afirma que "não havendo qualquer tipo de possibilidade de nós escrutinarmos a veracidade da notícia ou da informação, o que temos de fazer é projetar todos os cenários possíveis e aí seguramente nós nunca caímos na tentação de falhar".

Conclui-se daqui que no planeamento e preparação de eventos para os quais somos pressionados com inúmeras informações das quais não conseguimos verificar a sua veracidade, devem ser traçados cenários em conformidade com as informações recolhidas, não descartando qualquer possibilidade. "É prepararmo-nos para o pior e esperar o melhor", afirma Antunes, referindo ainda que "fala com os seus oficiais, dizendo que temos de nos preparar e traçar, claramente, todos os cenários a todos os níveis". Alves reforça que "no planeamento não temos a certeza que se vai realizar certo evento, mas ele tem de lá constar. Portanto, o planeamento

deve prever esse cenário e a resposta policial", caso o mesmo se venha a verificar. "Na ausência de informação não há outra solução", conclui Antunes. Constata-se, assim, que caso não se consigam validar todas as informações e todas as fontes disponíveis, devem ser elaborados cenários de reposta para a eventualidade destes eventos se virem a concretizar, mesmo considerando pouco provável que eles venham a ocorrer. Neste sentido, a PSP tem que estar pronta para intervir em qualquer situação, independentemente das informações que sejam recolhidas e verificadas.

As restantes subcategorias dizem respeito à gestão das Informações Policiais (C.1, 4,2%) e à Inteligência Policial (C.2, 4,2%) que consiste no processo de análise das informações. Relativamente as fontes de informações, Alves refere que "não só recorremos a fontes abertas, mas também as acompanhamos pela importância que têm nos dias de hoje", mas que a ação policial se "baseia em primeiro lugar, ou se quisermos em paralelo, com as informações que recebemos dos nossos serviços de inteligência". Antunes vai ao encontro da opinião de Alves e afirma que "uma das áreas a que sempre se recorre são as fontes abertas, mas depois estas têm de ser sempre reforçadas com as fontes humanas ou com outras fontes oficiais", como por exemplo o Departamento de Informações da PSP. Ainda refere que "de qualquer maneira a atividade da polícia, até por limitações legais, assenta quase na generalidade em fontes abertas", havendo, portanto, uma necessidade de escrutinar as fontes porque muitas delas não são verdadeiras. "Por exemplo, às vezes eles comunicam uma manifestação e dizem que vão ter 1000 participantes, embora a verdade é que nós já temos experiência nas redes sociais e em princípio, o número de *likes* corresponde em média aos participantes", sendo que os "números reais das pessoas nunca fogem muito do número de *likes* ".

Assim que obtemos informações provenientes de fontes abertas, "é determinado um esforço de pesquisa que se baseia quer em informações de outras polícias, quer em informações daquilo que se designa na nossa gíria policial como HUMINT, a fonte humana", acrescenta Antunes. Ainda e "também desmistificando, em termos policiais há cada vez mais aplicações que nos permitem fazer a conexão de todas as redes sociais para ver inclusivamente se aquelas informações são ou não *Fake news*", conclui Antunes.

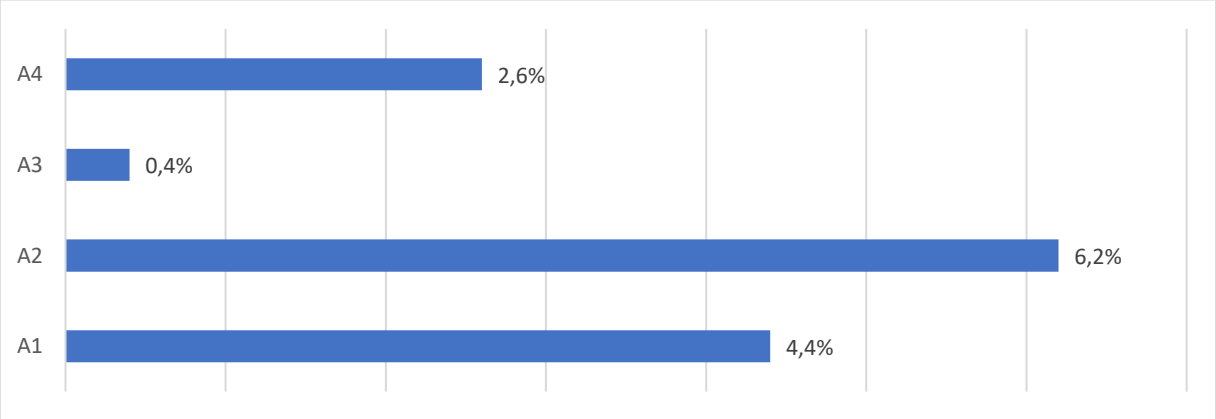
Na subcategoria da Inteligência Policial (C.2, 5,8%), vemos um grande enfoque no que é a análise das redes sociais, e o papel da Polícia na monotorização e análise permanente da

Internet. Antunes afirma que "em termos policiais não tem a mínima dúvida que acompanhamos um bocadinho a evolução tecnológica e abandonamos, em parte, a componente clássica, no entanto, nunca a podemos abandonar de todo. Em todo o caso, hoje temos uma presença na *Internet* muito superior que ronda a ordem dos 70%, sendo que todo o nosso esforço é canalizado para a monitorização das redes sociais". Face à necessidade de proceder a análise de fontes abertas, nomeadamente as redes sociais, podem surgir, "repercussões, desde logo, na análise dessa fonte de informação, constituindo um risco acrescido.

Por sua vez, Alves assume que "não há volta a dar, a PSP tem que acompanhar as redes sociais, e tem-no feito em determinados momentos de forma espetacular". Esta análise e esta presença é fundamental, uma vez que permite "acompanhar em paralelo o que circula nas redes sociais, ou até em alguns grupos mais privados a que vamos tendo acesso, para perceber as intenções do outro lado que possam condicionar o nosso trabalho". Antunes refere ainda que existe uma estratégia "de monitorização das redes e policiamento de toda a *Internet*", uma vez que quase todos os eventos têm uma "projeção muito potenciada pelas redes sociais". Não obstante, Alves afirma que "temos de nos apoiar na parte científica, com os nossos serviços de inteligência.". Antunes conclui afirmando que "neste momento vivemos num mundo de perceções, sendo que temos de colocar o máximo cuidado e a máxima prioridade na supervisão das redes sociais".

Figura 5

Distribuição percentual da subcategoria A



Nota. Elaboração própria com base na distribuição percentual da subcategoria A

A categoria A demonstra uma predominância nas subcategorias que dizem respeito à Desinformação (A.1, 4,4%) e à Manipulação da Realidade (A.2, 6,2%). Laranjo começa por referir que a desinformação "é um perigo que acontecerá sempre, sendo que o desafio é diminuir o erro". Esta ideia generalista demonstra, em parte, uma das grandes preocupações atuais inerentes ao crescimento exponencial das redes sociais. Ainda de acordo com Laranjo, existe uma grande quantidade de informações que são impactantes ao ponto de "conseguir criar imagens distorcidas da realidade". Ramos defende que o impacto da disseminação de *fake news* "depende da forma como são difundidas essas informações e do impacto que acabam por ter ou da importância que nós lhes damos". Por sua vez, Zamith refere que é "ainda mais complicado os cenários em que há mesmo atuação deliberada no sentido de passar *fake news*", dificultando o controlo e a monitorização destes atores que partilham e disseminam este tipo de informações. Ainda assim, "há sempre um pequeno grupo de pessoas que acredita sempre nas *fake news*", afirma Ramos, sendo que, na opinião de Zamith, a "sociedade vai-se cansar das *fake news* e vai-se cansar de ser enganado", acabando por desvalorizar cada vez mais a informação que circule nas redes sociais, privilegiando os OCS tradicionais.

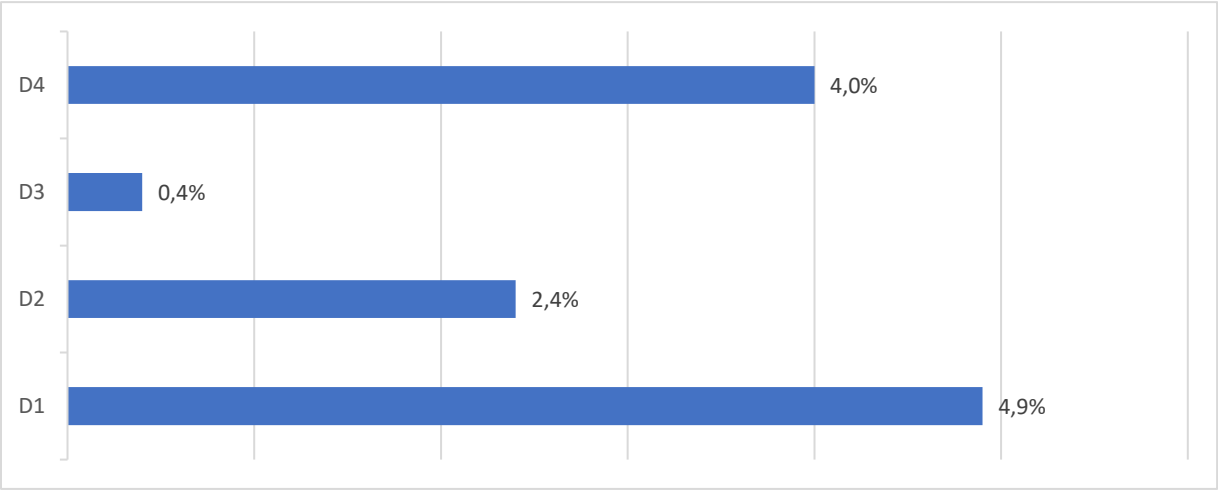
Importa ainda destacar outra característica predominante das *fake news*, que consiste na capacidade de mobilização que estas podem vir a ter. Ramos refere que "temos manifestações que são convocadas e que têm 10 milhões de aderentes em que não aparece ninguém, e temos desafios de claques que são feitos minutos antes dos jogos e, de repente, aparecem 100 indivíduos de cada lado e temos um problema de ordem pública" grave, e que as polícias têm que resolver. Estas notícias podem ser de tal modo agregadoras que acabam inclusive por "agrupar todos aqueles que estão descontentes" a manifestarem-se por motivos completamente distintos. Esta capacidade de mobilização é de todo potenciada pela "capacidade de mobilização das redes sociais" afirma Ramos, uma vez que estas conseguem fazer chegar, em minutos, informações a todos os cantos do mundo. Vivemos num mundo em que as *fake news* deixam de ser produzidas "por mera brincadeira de mau gosto, e tentam obter algum benefício pontual", conforme refere Zamith. Este dá-nos ainda alguns exemplos disto como "o de beneficiar com as subidas e descidas das ações na bolsa através da criação e disseminação de *fake news*" e das "campanhas políticas associadas à profissionalização de desinformação".

Relativamente à subcategoria que aborda a Desestabilização (A.3, 0,4%) provocada pelas *fake news*, e embora apresente uma menor predominância importa retirar algumas ideias relevantes. Antunes refere que "não tem a mínima dúvida de que algumas empresas tendem a, numa lógica de contrainformação, produzir nos destinatários uma instabilidade" de modo a retirar benefícios para os próprios, sendo que as notícias, mesmo quando são falsas, "conseguem gerar uma onde de escrutínio, nem que seja de escrutínio público", escrutínio este que pode contribuir para o aumento da instabilidade social.

À semelhança do que temos observado anteriormente, de um modo, geral a Resposta (A.4, 2,6%) às *fake news* deve depender das estratégias das entidades ou dos visados pela informação. Como constatamos anteriormente o facto de desmentir publicamente uma *fake new* está no fundo a "aumentar a visibilidade da mesma, chamando a atenção para aquele conteúdo, que se calhar algum do público não conhecia e vai passar a ver e aumentar a visibilidade para aquilo", afirma Zamith. O mesmo remata afirmando que esta escolha "tem um efeito perverso, e que é preciso ter algum cuidado com isso". A gestão do combate às *fake news* e à desinformação deve assentar num equilíbrio bastante difícil de alcançar. É preciso discernir entre desmentir uma *fake new*, ou deixar que o próprio tempo faça o seu trabalho, e acabe por fazer esquecer estes acontecimentos.

Figura 6

Distribuição percentual da subcategoria D



Nota. Elaboração própria com base na distribuição percentual da subcategoria D

No que diz respeito às redes sociais, as subcategorias que apresentam um maior número de U.r. são as referentes à Viralização (D.1, 4,9%) e à Gestão das Redes Sociais (D.4, 12,9%). Laranjo começa por afirmar que "a pressa é inimiga da perfeição e que, de facto, o mundo virtual trouxe uma correria à informação". Neste sentido, Antunes refere que "o que lhe parece é que as *fake news* atingem uma determinada dimensão em função da sociedade digital" e da facilidade de acesso a esse mundo digital. Ramos dá-nos o exemplo da situação atual que está a ocorrer na Ucrânia, em que as informações que circulam principalmente no *twitter* e que "parecem fidedignas que estão a acontecer de um lado e do outro, são na realidade os *sides* de ambos os lados que estão a manipular a opinião pública à escala global". Zamith alerta para o facto de que inclusive algo "possa ter sido publicado e afinal não estava correto, mas, no entanto, já fez alguma mossa, como se costuma dizer. Já teve os seus efeitos, já houve gente que leu e que viu e depois pode até nem ter visto o comunicado a desmentir e fica com essa ideia".

Transversalmente os nossos entrevistados fazem alusão à necessidade de garantir uma regulação efetiva e eficaz das redes sociais. Relativamente ao acesso às redes sociais, Zamith refere que "na internet estabelecemos também as nossas redes sociais, partilhamos alguma coisa com aquelas pessoas, partilhamos alguma coisa em comum, ou temos alguma coisa que nos identifica, por isso é que estamos em cada uma daquelas redes", sendo que o acesso a estas é um processo super facilitado e acessível a todos. Ramos começa por referir que "ninguém controla rigorosamente nada do que é publicado em termos de *fake news* nas redes sociais" e que "tem que existir efetivamente um controlo e temos que colocar isto no centro do palco".

Para Zamith uma forma de atenuar a disseminação de *fake news* nas redes sociais é uma "medida mais drástica, mas legal, que é banir um site, expulsar aquilo ou aqueloutro". "Imaginando que um utilizador de uma plataforma qualquer é responsável pela produção de uma *fake new*, entendo como legítimo que aquela pessoa seja expurgada". Acrescenta ainda que pode inclusive "haver legislação para isso, podendo haver até atuação do poder judicial para tomar essa decisão". Ramos refere ainda que "as redes sociais necessitam de uma regulação eficaz, não de censura" e que é "completamente inconcebível que à escala global as redes sociais continuem com toda esta possibilidade de nos induzir a ir para becos sem saída".

De um modo geral, deve haver uma aposta que incida na regulação das redes sociais para que se evite que os mesmos atores continuem constantemente a produzir e disseminar

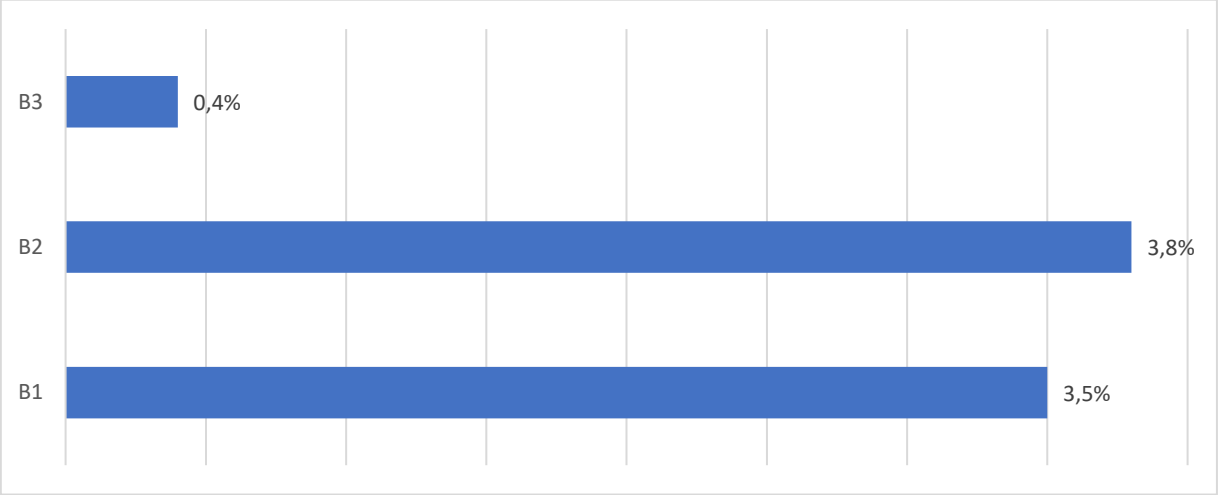
desinformação, identificando-os e punindo-os. A única forma de controlar as "redes sociais passa por uma fortíssima regulação das mesmas, que nesta altura são a completa selva", conclui Ramos.

Nas restantes subcategorias, avaliamos a Perceção (D.2, 2,4%) que as pessoas têm das redes sociais e a necessidade de garantir a Confirmação (D.3, 0,4%) da veracidade das informações que circulam nestes meios. Alves começa por referir que não "podemos esquecer-nos de que o mundo digital existe e que o mundo digital tem muito poder", pelo que "não se pode ignorar a importância do mundo virtual e deve ter-se em conta toda a perceção das pessoas para poder reenquadrar os factos", afirma Laranjo. Zamith esclarece que "as redes sociais somos nós que as fazemos com as pessoas com quem nos ligamos cada vez que nos inscrevemos numa plataforma" pelo que é óbvio que "estamos sempre a falar de um mundo de perceções."

Contudo, e de acordo com Antunes, "quando falamos de perceções essa informação nem sempre vai para as pessoas com mais recursos técnicos". No que diz respeito à confirmação da veracidade das informações que circulam nas redes sociais, e conforme temos vindo a referir, as redes sociais podem ser uma excelente ferramenta de recolha e consulta de informação. Não obstante, deve ser feito um esforço paralelo, de modo a tentar perceber se a informação que está a ser consultada é efetivamente verídica ou não. Laranjo refere que "também usa as redes sociais, mas sempre com um sentido crítico de que as mesmas não tiveram de ser contraditadas", pelo que esse trabalho tem que ser feito individualmente. A mesma acrescenta que "valoriza as redes sociais", contudo "segue-as e valida-as" antes de poder usar a informação que lá esteja vertida.

Figura 7

Distribuição percentual da subcategoria B



Nota. Elaboração própria com base na distribuição percentual da subcategoria B

Por último, na categoria B, encontramos uma predominância de U.r. semelhante nas subcategorias que dizem respeito ao Controlo da Informação (B.1, 3,5%) e à Partilha de Informação (B.2, 3,8%). Laranjo começa por afirmar que "um leitor informado é alguém que consegue destrinçar o certo do errado e o que consegue distinguir informação de desinformação". Neste sentido, Antunes afirma "que o impacto da desinformação é medido de acordo com o destinatário, uma vez que há coisas que à partida eu sei perfeitamente identificar, pela gama de conhecimentos que tenho que aquilo é *fake new*". Este adianta que obviamente que "para combater a contrainformação, só é possível com a credibilidade da informação" e a verificação das fontes.

Zamith aborda a temática explicando que, "com a falta de literacia mediática que uma grande parte da população tem, de não ter capacidade e aptidão para distinguir o que é uma fonte credível de uma fonte não credível", devem ser tomas medidas no sentido de informar e sensibilizar a população para os perigos que advêm da desinformação e algumas formas de a contrariar. Devem ser adotadas "práticas e alertar a população para que olhe duas vezes, pense duas vezes, verifique, recorra a outras fontes e não acredite na primeira coisa que lhe aparece à frente".

No fundo, constatamos uma necessidade de incutir na população em geral uma autodisciplina da verificação da informação que circula no ciberespaço. Zamith refere a existência de "uma outra iliteracia mediática, no que diz respeito ao jornalismo, que é tanta que imensa gente confunde o jornalismo com algumas coisas parecidas que andam na internet, sobretudo nas redes sociais, que veio baralhar ainda mais a população". Assim, este refere que podem e devem ser feitas "todas as ações e mais algumas que alertem a sociedade, que dêem instrumentos e formação à sociedade no seu todo, para ficar mais desperta para esta realidade", admitindo ainda a possibilidade de criar plataformas que as pessoas possam consultar "e fazer uma autoformação que já ganhavam muito com isso".

A subcategoria que diz respeito às Informações Sensíveis (B.3, 0,4%) diz respeito a um conjunto de informações que por serem mais reservadas podem causar transtornos para terceiros, pelo que não foi algo a que os nossos entrevistados tenham atribuído muita importância. Laranjo referiu-nos, a título de exemplo, um suicídio que "por norma não é noticiado pelos jornalistas por vários motivos" de natureza ética, evitando mediatizar este tipo de situações.

Conclusão

O panorama securitário, nacional e internacional é, nos dias de hoje, marcado por uma elevada instabilidade, incerteza e imprevisibilidade. Neste contexto as *Fake News* assumem uma preocupante preponderância no âmbito da desinformação, tendo um potencial impacto na ordem pública. Como pudemos constatar, o desenvolvimento tecnológico e a maior facilidade de acesso a instrumentos eletrónicos veio desenvolver e potenciar um conjunto de novos mecanismos de comunicação de larga escala. O desenvolvimento e criação de redes sociais abriu a porta um novo universo no mundo da comunicação, facilitando este processo.

Uma vez que o acesso a estas redes sociais é livre e facilitado, verificamos que existem cada vez mais fluxos de informação partilhados. Contudo, estes fluxos de informação nem sempre se traduzem em fluxos de informação correta, pelo que é de todo pertinente detetar as fontes de informação falsa.

Conforme concluem os nossos entrevistados, a falta de controlo e de uma regulação eficaz das redes sociais possibilita que existam inúmeros agentes, cada vez mais profissionalizados, a operar nestas redes com um propósito único de causar instabilidade ou adquirir vantagens sobre terceiros. Existe uma premente necessidade de criar mecanismos capazes de auxiliar na deteção destes *Fake News* e garantir que a informação correta chega a toda a sociedade.

Aos OCS está incumbida a missão de auxiliar neste processo de deteção e desconstrução de *Fake News*. A criação de programas de *Fake Checking* e o *streaming* dos mesmos em horário nobre auxilia o cidadão no processo de *vetting check* da informação, desmentindo muitas das informações virais que surgem das redes sociais. Ainda, os nossos entrevistados não colocam de parte a possibilidade e a necessidade de evitar que se aumente a visibilidade de algumas destas *Fake News*, uma vez que o facto de as publicitarem, ainda que com o propósito de as desmentirem, pode aumentar a sua visibilidade e gerar uma onda de partilhas.

Ainda assim, e pelo elevado número de *Fake News* que são diariamente disseminadas, o controlo e monotorização destes atores que partilham e disseminam este tipo de informações

é praticamente impossível, obrigando a própria sociedade a ter capacidade de discernimento entre o que é falso e o que é factual e verdadeiro. A promoção de campanhas de formação e de ações de sensibilização na comunidade deverá ser uma medida adotada, com o intuito de aumentar o grau de literacia mediática de toda a sociedade.

A dificuldade de resposta às ameaças híbridas, em concreto as *Fake News*, advém da dificuldade de prever e de determinar eventuais danos que estas possam provocar. A complexidade da determinação dos danos que estas ameaças possam causar impossibilita a mitigação ou redução destes, uma vez que estes danos são muitas vezes colaterais, e impactam diretamente com a segurança e a ordem pública.

Enquanto ator responsável, a PSP tem o dever de garantir e assegurar a tranquilidade e a ordem pública, sendo este um dever legalmente atribuído, no artigo 272º da CRP. Neste sentido, a PSP deve conseguir adaptar-se à realidade e garantir respostas eficazes às novas ameaças à segurança.

A preparação e o planeamento da segurança de grandes eventos exigem um meticuloso esforço de pesquisa de modo a garantir que se recolhe o maior número de informação possível, construindo um planeamento completo, rigoroso e adequado. Devido à dimensão e complexidade destes eventos e à possibilidade de interferirem diretamente com o normal decorrer da vida em sociedade, devem ser tidas em conta todas as ameaças, riscos e vulnerabilidades que possam afetar ou interferir com a tranquilidade e a ordem pública, adequando o planeamento face às circunstâncias e informações disponíveis.

De acordo com os nossos entrevistados, é inevitável recolher dados de fontes abertas, uma vez que estas são cada vez mais utilizadas e comportam cada vez mais fluxos de informação. Deste facto resultam problemas associados à credibilidade das fontes, à diversidade de informação e à dificuldade de perceber a veracidade das mesmas, o que pode constituir um grave problema para a atividade operacional das Polícias.

A utilização de eventuais *Fake News* na construção de um planeamento pode enviesar o processo decisório e o comando e controlo de operações policiais. Os nossos entrevistados referem que é necessário dar uma réstia de verdade a todo o tipo de informações, sendo para tal

necessário contar com um cenário para essas informações. A falta de informações, ou a falta de confirmação sobre a veracidade das mesmas obriga as Polícias a serem flexíveis no seu planeamento, e a abandonar estratégias estanques e herméticas. Embora exista um risco acrescido na análise de fontes abertas (OSINT), nomeadamente das redes sociais, não podemos deixar de as incorporar enquanto fontes de informação no âmbito do CPI.

Através da análise das entrevistas concluímos que a estratégia de comunicação da PSP, no que diz respeito à intervenção perante *Fake News*, deve ser o mais equilibrada possível, sendo que a PSP deve estar presente e ser proativa nas redes sociais. Não podemos esquecer que o mundo digital está cada vez mais complexo e a ganhar cada vez mais relevância, pelo que a presença das polícias nestas redes pode ajudar a garantir um primeiro contacto mais próximo com o cidadão e intervir no esclarecimento de algumas *Fake News* que possam pôr em causa a segurança pública e a imagem ou a atividade da PSP. Decorrente do atrás referido, devem ser ponderadas várias ações possíveis, nomeadamente despoletando ações de natureza judicial nas circunstâncias que se justifiquem, a intervenção junto dos OCS e das redes sociais, para esclarecer os factos, desmentir eventuais fraudes ou mesmo garantir que determinados atores sejam excluídos das redes sociais.

Considerando ainda o facto das *Fake News* terem uma grande capacidade agregadora e de mobilização evidenciamos que em certos fenómenos, como o é o caso das reuniões e manifestações promovidas por movimentos inorgânicos, as informações disponíveis muitas vezes não coincidem com a realidade. Os entrevistados referem que, em bastantes eventos o número de pessoas, assim como os horários e os locais de concentração e tempo de duração do protesto que são divulgados não coincide com os dados pesquisados e recolhidos nas redes sociais pelas Forças e Serviços de Segurança. Apesar da predominância e da diversidade de fontes de informações abertas, devem ser privilegiadas fontes seguras, como as fontes humanas, e os produtos de inteligência dos serviços de inteligência da PSP.

Retomando a problemática da nossa investigação, concluímos que efetivamente as *Fake News* possuem um impacto na segurança e na ordem pública, que pode ser direto ou indireto. Existe uma necessidade de garantir que existe uma monotorização permanente das informações disponíveis em fontes abertas, e de tentar identificar eventuais atores que se

dediquem à disseminação deste tipo de informações, com o objetivo de causar impactos negativos na ordem e segurança públicas ou de instigar à prática de crimes.

A forma de mitigar eventuais danos passa pela cenarização, com base em todas as informações disponíveis. Sempre que não se consiga confirmar a veracidade das informações devem ser traçados cenários hipotéticos onde estejam estabelecidas todas as medidas a adotar, caso aquela informação se venha a verificar. Este processo deve ser sistematizado para todas as informações, uma vez que no planeamento da segurança de grandes eventos deve ser prevista uma infinidade de cenários e a resposta padrão da Polícia para cada um deles.

O combate à desinformação contraria-se com um planeamento e preparação rigorosos. A preparação destes cenários garante que não sejam menosprezadas algumas variáveis que podem influenciar a fase de execução das operações, minimizando os riscos de se verificarem falhas nesta mesma fase.

Concluímos ainda que a necessidade de adaptação e o desafio constante de detetar e intercetar *Fake News*, obriga a que seja feito um esforço permanente no sentido de acompanhar as mudanças que a sociedade sofre.

Esta dissertação foi afetada por algumas limitações, que nos causaram algumas dificuldades. A atualidade do tema e a falta de consenso da doutrina na conceptualização de alguns conceitos dificulta a exposição dos mesmos. Relativamente à bibliografia, verificamos que já começa a surgir bastante informação relacionada com a problemática das *Fake News*, mas que ainda não está muito direcionada para os impactos ao nível securitário, estando focalizada, no geral, para os impactos aos níveis sociais e políticos.

Uma vez que as fake news estão cada vez mais associadas às ciências policias e tendo em consideração que estas podem produzir um conjunto de impactos diretos e indiretos para a segurança e ordem pública, devem ser desenvolvidos futuros estudos nestas áreas.

Por último e para investigações futuras, deixamos a sugestão do desenvolvimento de estudos sobre a implementação de sistemas (recorrendo, por exemplo, à inteligência artificial) que sejam capazes de identificar automaticamente na rede, as informações importantes para o planeamento da segurança de grandes eventos e estudar a sua aplicabilidade na Polícia de

Segurança Pública. Por exemplo, um *software* que detete grupos ou pessoas que convoquem ações nas redes sociais, com o objetivo de perturbar a segurança e ordem pública durante grandes eventos, facilitaria o trabalho de recolha e análise das informações e constituir-se-ia como uma ferramenta essencial para o planeamento policial.

Da mesma forma, será importante a PSP estabelecer mecanismos de policiamento e de análise das redes sociais, antes durante e depois das operações policiais em grandes eventos, para detetar narrativas falsas que tentem deslegitimar a ação das Forças de Segurança, como foi o caso de algumas ações de desinformação no período da Troika em Portugal.

No entanto, temos consciência que a adoção destes sistemas automatizados que emitam alertas, não poderá restringir direitos constitucionais, como a liberdade de expressão, reunião e manifestação, nem pode ser utilizado para outros fins que não a prevenção ou investigação criminal.

Finalmente, sugerimos que possam ser ainda desenvolvidos estudos de caso em que se analisem algumas das maiores operações de segurança de grandes eventos dos últimos anos, verificando se foram detetadas ou não *Fake News* durante o processo de planeamento e execução e determinando o seu impacto na atividade policial e na segurança dos cidadãos.

Referências

Aldwairi, M., & Alwahedi, A. (2018, novembro 5- novembro 8). Detecting fake news in social media networks [Sessão de conferência]. *The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks* (EUSPN 2018), Bélgica.

Altheide, D., & Snow, R. (1979). Media Logic. Sage.

Arcos, R., & Smith, H. (2021). Digital communication and hybrid threats. Presentation. *Icono 14, 19*(1), 1-14. https://doi.org/10.7195/ri14.v19i1.1662

Bachmann, S., & Gunneriusson, H. (2015). Hybrid wars: The 21st-century´s new threats to global peace and security. *Scienta Militaria South African Journal of Military Studies, 43*(1), 77-92. https://doi.org/10.5787/43-1-1110

Baines, P., O´Shaughnessy, N., & Snow, Nancy. (2020). *The sage handbook of propaganda*. Sage

Bardin, L. (2016). *Análise de conteúdo* (3ª ed.). Almedina

Bauman, Z. (2006). *Confiança e medo na cidade*. Relógio d'Água.

Beccaria, C. (2007). *Dos delitos e das penas*. Fundação Calouste Gulbenkian.

Bogdan, R. C., & Bilken, S. K. (1994). *Investigação qualitativa em educação*. Porto Editora

Bouças, C., Carvalho, V., Gabriel, I., Loureiro, J., & Ribeiro, M. (2020). *Comunicação e defesa nacional: Impacto das fake news na defesa nacional. Contributos para medidas de mitigação* [Curso de Defesa Nacional, Instituto de Defesa Nacional]. Instituto Defesa Nacional.

Breakspear, A. 2013. A new definition of intelligence. *Intelligence and National Security, 28*(5), 678-93. https://doi.org/10.1080/02684527.2012.699285.

Camargo, I., & Bradshaw, S. (2021). Disinformation 2.0: Trends for 2021 and beyond. *Hybrid CoE, 11*(1), 3-28. https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf

Carmo, H. (2013). *Sistemas de orientação na pesquisa: Formulação de objetivos, hipóteses e modelo de análise. Manual de metodologia das ciências sociais e políticas*. ISCSP/UTL.

Castells, M. (2012). *A sociedade em rede. A era da informação: Economia, Sociedade e Cultura* (Volume I). Fundação Calouste Gulbenkian.

Clemente, P. (2015). *Cidadania, Polícia e Segurança Pública*. ISCPSI.

Comissão Europeia. (2018, 13 junho). Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas [Sessão de Conferência]. *Comunicação conjunta ao Parlamento Europeu, ao Conselho Europeu e ao Conselho*, Bruxelas.

Consentino, G. (2020). Social media and the post-truth world order: The global dynamics of disinformation (1ª ed.). Palgrave Pivot. https://doi.org/10.1007/978-3-030-43005-4.

Corbe, M., & Cusumano, E. (2018). *A civil-military response to hybrid threats*. Palgrave Macmillan.

Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: Covert action anda implausible deniability. *International Affairs, 94(3)*, 477-499. https://doi.org/10.1093/ia/iiy067

Decreto de 10 de abril de 1976. Diário da República n.º 86/1976 – Série I. Lisboa: Presidência da República, 738-775.

Delgado, A., Torres, M., Ortega, V., Torres, J., Fernándes-Montesinos, F., Gil, E., & Gutiérrez, F. (2021, 30 junho). La desinformación como soporte de las narrativas. *Jornadas académicas informativas, 1*(1), 1-56. https://www.policefitness.es/wp-content/uploads/2022/01/IDIT-URJC.pdf

Derakhshan, C. (2018). Thinking about 'information disorder': Formats of misinformation, disinformation, and mal-information. Em C. Ireton, & J. Posetti (Eds.), *Journalism, 'fake news' and disinformation: A handbook for journalism education and training* (pp. 43-54). UNESCO. https://en.unesco.org/sites/default/files/f._jfnd_handbook_module_2.pdf

Elias, L. (2018). *Ciências policiais e segurança interna: Desafios e prospetivas*. ISCPSI.

Elias, L. (2019). O terrorismo transnacional contemporâneo: Segurança, justiça e cooperação. *Nação e Defesa, 152*(1), 78-112.

https://comum.rcaap.pt/bitstream/10400.26/32222/6/ELIASLuis_Oterrorismotransnacionalcontempor%C3%A2neo_ND_152_p_78_112.pdf

Fallis, D. (2015). What is Disinformation? *Library Trends, 63*(3), 401-426. https://doi.org/10.1353/lib.2015.0014

Fernandes, L. F. (2014). *Intelligence e Segurança Interna*. ISCPSI.

Fortin, M. F. (2009). *O Processo de investigação: Da conceção à realização* (5ª ed.). Lusociência.

Freedman, J., Gjørv, G. H., & Razakamaharavo, V. (2020). Identity, stability, hybrid threats and disinformation. *Icono 14, 19*(1), 38-69. https://doi.org/10.7195-ri14.v19i1.1618

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world* (3ª ed.). War & Peace Studies.

Gill, P., Marrin, S., & Phythian, M. (2008). *Intelligence theory: Key questions and debates*. Routledge Taylor & Francis Group.

Gottfried J., & Shearer, E. (2016, maio 6). News use across social media platforms 2016. *Pew Research Center*. https://www.pewresearch.org/journalism/2016/05/26/news-use-across-social-media-platforms-2016/

Guess, A. M., & Lyons, B. A. (2020). *Misinformation, disinformation and online propaganda*. Em Persily, N., & Tucker, J. A. (Eds.). *Social Media and democracy: The state of the field and prospects for reform* (pp. 10-33). Cambrige University Press.

Inteligência (2022, 15 de janeiro). In *Infopédia*. https://www.infopedia.pt/dicionarios/lingua-portuguesa/inteligencia.

Ivanjko, T. (2019). *Open sources intelligence (OSINT): Issues and trends*. University of Zagreb.

Johnson, L. K. (2009). Sketches for a theory of strategic intelligence. Em P. Gill, S. Marrin, & M. Phythian (Eds.). *Intelligence theory: Key questions and debates* (pp. 33-53). Routledge Taylor & Francis Group.

Jowett, G., & O'Donnel, V. (2015). *Propaganda and Persuasion*. Sage.

Korta, S. M. (2018). *Fake news, conspiracy theories, and lies: An information laundering model for Homeland security* [Dissertação de Mestrado, Naval Postgraduate School]. Monterey, California.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Towards an interdisciplinary framework for research and policy making*. Council of Europe

Larsen, A. J., & Lasconjarias, G. (2015). *NATO's response to hybrid threats*. Nato Defense College.

Lei n.º 53/2008, de 28 de agosto. *Diário da República n.º 167/2008 – Série I*. Lisboa: Assembleia da República, 6135-6141.

Liu, H., & Shu, K. (2019). *Detecting fake news on social media*. Morgan & Claypool Publishers.

Marconi, M. A., & Lakatos, E. L. (2017). *Fundamentos de metodologia científica* (8ª ed.). Editora Atlas.

Maro, S., Steghofer, J., Hayes, J., Cleland-Huang, J., & Chalmers, M. (2018). Vetting automatically generated trace links: What information is useful to human analysts? [Sessão de Conferência]. *26th International Requirements Engineering Conference*, Suécia.

Marrin, S. (2009). Intelligence analysis and decision-making: Methodological challenges. Em P. Gill, S. Marrin, & M. Phythian (Eds.). *Intelligence theory: Key questions and debates* (pp. 131-150). Routledge Taylor & Francis Group.

Nagasako, T. (2020). Global disinformation campaigns and legal challenges. *International Cybersecurity Law Review, 1*(1), 125-136. https://doi.org/10.1365/s43439-020-00010-7

NEP n.ºAUOOS/DO/01/24 de setembro de 2016. Lisboa: Direção Nacional da PSP.

NEP n.º AUOOS/DIP/02/05/30, de dezembro de 2014. Lisboa Direção Nacional da PSP.

Newman, N., Fletcher, R., Schulz, A., Andi, C., Robertson, C., & Nielson, R. (2021). *The Reuters institute digital news report 2021* (10ª ed.). Reuters Institute for the Study of Journalism.

Nougayrède, N. (2018, 31 janeiro). In this age of propaganda, we must defend ourselves. *The Guardian*. https://www.theguardian.com/commentisfree/2018/jan/31/propaganda-defend-russia-technology

Omand, D. (2010). *Securing the State*. Oxford University Press.

Omand, D., Jamie B., & Millet, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823. https://doi.org/10.1080/02684527.2012.716965

O´Shaughnessy, N. (2020). *From disinformation to fake news: Forwards into the past*. Em Baines, P., O´Shaughnessy, N., & Snow, N. (Eds). *The sage handbook of propaganda*. (pp. 55-70). Sage

Paul, A., Izewicz, P., Flatow, G., Bachmann, S., Gunerisusson, H., & Bowen, A. (2014). The journal on terrorism and security analysis. *Spring*, *9*(1), 27-36.

Pereira, J. (2018). As ameaças híbridas – Uma abordagem conceptual no quadro da OTAN e da UE. *Direito Segurança e Democracia*, *60*(1), 1-25.

Persily, N., & Tucker, J. A. (2020). *Social Media and democracy: The state of the field and prospects for reform*. Cambrige University Press.

Peterson, M. (2020). The evolutionary psychology of mass mobilization: How disinformation and demagogues coordinate rather than manipulate. *Current Opinion in Psychology, 35*(1), 71-75. https://doi.org/10.1016/j.copsyc.2020.02.003.

Planeamento (2022, 15 de janeiro). In *Infopédia*. https://www.infopedia.pt/dicionarios/lingua-portuguesa/planeamento

Quivy, R., & Campenhoudt, L. V. (2017). *Manual de investigação em ciências sociais* (5ª ed.). Gradiva.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Willian Publishing.

Reis, P. (2017). A tomada de decisão dos comandantes de polícia em grandes eventos políticos [Dissertação de Mestrado, ISCPSI]. *Repositórios Científicos de Acesso Aberto de Portugal*. http://hdl.handle.net/10400.26/19930

Ribeiro, N. (2021). Desinformação online: O impacto da propaganda participativa. *Oração de Sapiência proferida na Sessão Solene do Dia Nacional da UCP, 2021*. Universidade Católica.

Sari, A. (2020). *Hybrid threats and the law: Concepts, trends and implications* [Relatório]. Hybrid CoE Trend Report 3.

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

Severino, A. (2017). *Metodologia do trabalho científico* (24ª ed.). Cortez editora.

Shu, K., Wang, S., Lee, D. & Liu, H. (2020). Mining disinformation and fake news: concepts, methods, and recent advancements. Em K. Shu, S. Wang, D. Lee, & H. Liu (Eds.), *Disinformation, misinformation, and fake news in social media* (pp. 1-19). Springer.

Silverman, D. (2009). *Interpretação de dados qualitativos: Métodos para a análise de entrevistas, textos e interações* (3ª ed.). Sage.

Taleb, N. N. (2020). *O cisne negro: O impacto do altamente improvável*. D. Quixote.

Tandoc, Jr., E., Lim, Z., & Ling, R. (2017). Defining "fake news". *Digital Journalism*, *6*(1), 137-153. https://doi.org/10.1080/21670811.2017.1360143

Treverton, G. F. (2018). *The intelligence challenges of hybrid threats: Focus on cyber and virtual realm*. Center of Asymmetric Threat Studies.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). *Addressing hybrid threats*. Swedish Defence University.

Tzu, S. (2015). *A arte da guerra* (M. Robalo & M. Mata, Trads.; 1a ed.). Edições Sílabo. (Trabalho original publicado 1910).

Van de Weert, A., Rottweilwe, B., Wchmann, F., Farinelli, F., Gill, P., Lewandowsky, S., & Analyst M. (2021). *Conspiracy narratives & disinformation*. Spotlight.

Vasconcelos, A. (2009). *Between sel-interest and a "responsible-power" aproach*. Em F. Zhongping, R. Hutchings, R. Kumar, E- Sidiropoulos, P. Wrobel, & A. Zagorski (Eds.), Global security in a multipolar world (pp. 5-134). Institute for Security Studies

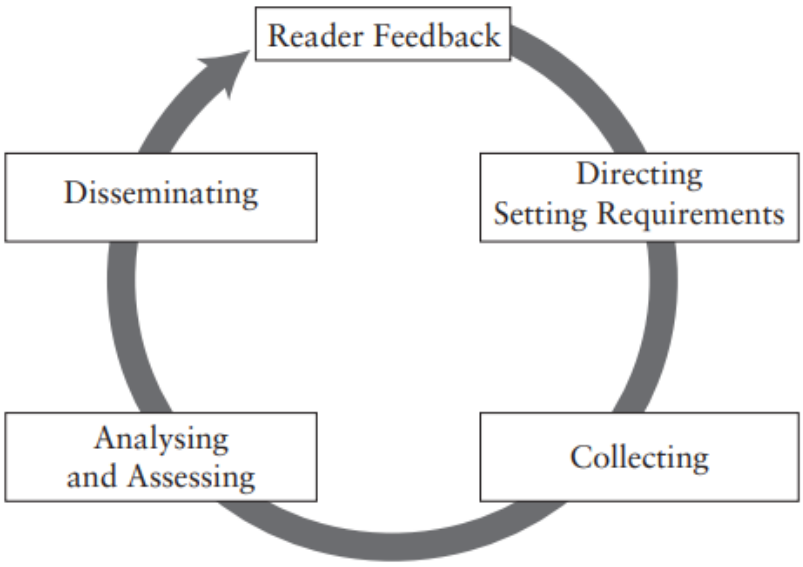
Vasu, N., Ang, B., Teo, T., Jayakumar, S., Faizal, M., & Ahuja, J. (2018). *Fake news: national security in the post-truth era*. Nanyang Technology University Singapore.

Vosoughui, S. Roy, D., & Aral, S. (2018). The Spread of True and False News Online. *Science, 6380*(359), 1146-1151.

Wilderbeek, F. (2021). El seguimiento sobre las fake news en medios institucionales durante el coronavirus en España. *Vivat Academia: Revista de Comunicación, 154*(1), 1-12. https://doi.org/10.15178/va.2021.154.e1253

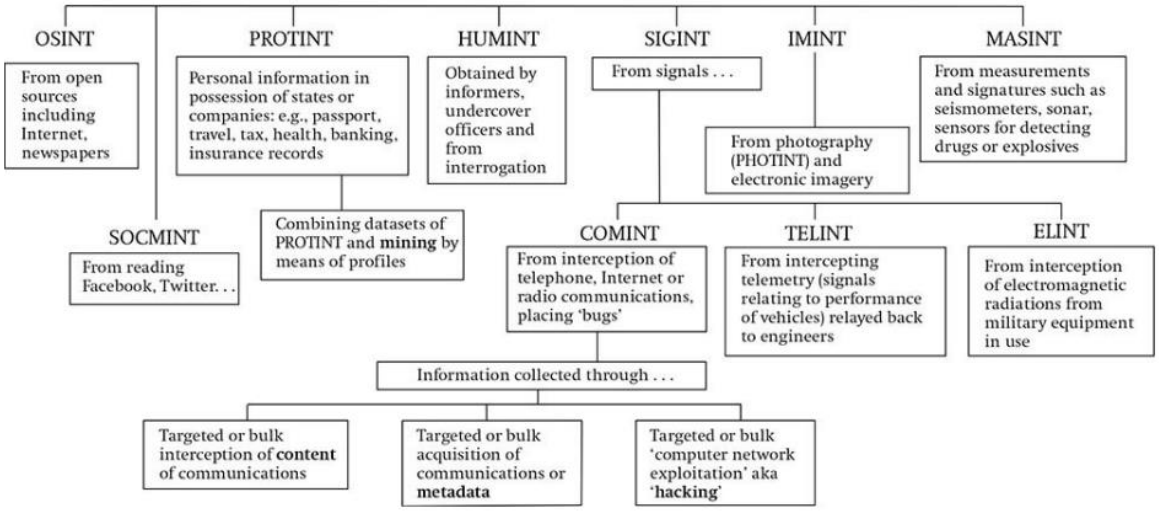
Anexos

Anexo 1- Ciclo de Produção de Inteligência (Omand, 2010)



Fonte: Adaptado de "Securing the State" de D. Omand, 2010, Oxford University Press., p. 118. Copyright 2010 de Oxford University Press

Anexo 2- Fontes de Inteligência (Gill e Phytian, 2018)



Fonte: Adaptado de "Intelligence in na insecure world (3ª ed.)" de P. Gill, & M. Phythian, 2018, War & Peace Studies. s.p. Copyright 2018 de War & Peace Studies.

Apêndices

Apêndice A- Guião de Entrevista Externo

Guião de Entrevista subordinado ao tema:

O Impacto das *Fake News* na Segurança e Ordem Pública

1. Consideram que as *Fake News* são suficientemente impactantes para modificar as opiniões dos cidadãos? Qual o impacto destas *Fake News* na construção de uma imagem/ideia/credo?

2. Considera que existem campanhas construídas propositadamente para conseguir objetivos baseados em *Fake News*?

3. Acha necessário que as entidades/instituições reajam perante as *Fake News*? Qual a melhor estratégia para minimizar/mitigar o impacto das mesmas?

4. Atendendo a diversidade de fontes de informações, de que modo vê a posição dos OCS perante a mediatização de notícias através das redes sociais?

5. No exercício da sua atividade profissional, já teve que tomar decisões, ou alterar estratégias face a informações surgidas nas redes sociais? Como enquadra as *Fake News* numa perspetiva deontológica?

6. Estando numa linha da frente em matéria de produção de informação, de que modo opta pela escolha das fontes de informação (Redes sociais ??)?

7. Qual a sua posição se verificar que uma notícia que se tornou viral e não tendo possibilidade de verificar a sua autenticidade?

8. Atendendo à dimensão de que as *Fake News* podem tomar, de que modo é que consegue atenuar o impacto das mesmas?

9. De que forma integra as informações produzidas nas redes sociais no planeamento e decisões no âmbito da sua atividade profissional?

10. No âmbito das suas funções qual a importância atribuída às redes sociais na gestão corrente?

11. Como gere o risco de publicitação de uma notícia que não é 100% segura?

Apêndice B – Guião de entrevista policial

Guião de Entrevista subordinado ao tema:

O Impacto das *Fake News* na Segurança e Ordem Pública

1. Consideram que as *Fake News* são suficientemente impactantes para modificar as opiniões dos cidadãos? Qual o impacto destas *Fake News* na construção de uma imagem/ideia/credo?

2. Considera que existem campanhas construídas propositadamente para conseguir objetivos baseados em *Fake News*?

3. Acha necessário que as entidades/instituições reajam perante as *Fake News*? Qual a melhor estratégia para minimizar/mitigar o impacto das mesmas?

4. Atendendo a diversidade de fontes de informações, de que modo vê a posição dos OCS perante a mediatização de notícias através das redes sociais?

5. No exercício da sua atividade profissional já teve que tomar decisões , alterar estratégias ou táticas de policiamento face a informações falsas ou adulteradas surgidas nas redes sociais?

6. No âmbito das suas funções profissionais qual a importância que atribui às redes sociais na gestão corrente da atividade policial?

7. Na fase de planeamento recorre a informações obtidas em fontes abertas? Se sim como é que garante a fiabilidade das mesmas?

8. Perante a eminência da realização de um grande evento e face à impossibilidade de confirmar em tempo útil as informações produzidas através das redes sociais, qual a estratégia recomendada no âmbito da garantia da ordem e da segurança pública? Existe alguma forma de retirar informação através das *Fake News*?

9. Qual a estratégia institucional para reagir a *Fake News* negativas para a imagem institucional? Entende que a PSP tem que reagir institucionalmente a todas as *Fake News* ou haverá situações onde o senso comum fará essa "defesa da honra" institucional sem necessidade de reação formal?

Apêndice C – Termo de consentimento informado

Tomei conhecimento que o 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 Mário Rui Gonçalves Pereira, está a desenvolver um estudo sobre o impacto das fake news na segurança e ordem pública, sob orientação do Prof. Doutor e Superintendente Luis Elias e sob a coorientação do Prof. Doutor e Superintendente Leitão da Silva. 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 gravadas para facilitar a sua análise, sendo destruídos os registos áudio após a sua transcrição. A minha colaboração tem carácter voluntário, podendo desistir em qualquer momento do trabalho.

A minha participação neste inquérito não implicará qualquer remuneração ou custo associado. 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.

O investigador

_____

Aspirante a Oficial de Polícia

M/157268

O(a) entrevistado(a)

_____

_____

Lisboa, ____ de _____ de 20__

Apêndice D – Autorização realização de entrevistas

POLÍCIA SEGURANÇA PÚBLICA

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

DIRECÇÃO DE ENSINO

SECRETARIA ESCOLAR

Exmo. Senhor
Diretor Nacional Adjunto/Unidade Orgânica de Recursos Humanos
(Departamento de Formação)
DN/PSP Largo da Penha de França, N.1
1199-010 LISBOA

Sua Referência:
Sua Comunicação:
Nossa Referência: 29/SECDE/2022
Classificador: 080.01.10
Processo: SECDE202100001ASP
Data: 2022-01-17

Assunto: PEDIDO DE COLABORAÇÃO EM TRABALHO DE DISSERTAÇÃO DE MESTRADO INTEGRADO EM CIÊNCIAS POLICIAIS

1. O Curso de Mestrado Integrado em Ciências Policiais (CMICP), no 5.º ano - Estágio, compreende a elaboração de uma dissertação/trabalho de projeto que deverá, obrigatoriamente, incidir sobre um tema das áreas científicas de ciências policiais, ciências jurídicas e ciências sociais e humanas.
2. O Aspirante a Oficial de Polícia Mário Rui Gonçalves Pereira irá realizar o seu estudo numa daquelas áreas científicas, subordinado ao tema "O Impacto das Fake News na Segurança e Ordem Pública", do qual são orientadores o Sr. Superintendente Luís Elias e o Sr. Superintendente António Leitão da Silva.
3. Tem-se por objetivo perceber a temática das Fake News, nomeadamente sobre o impacto destas ameaças na fase de planeamento de grandes eventos, e sobre possíveis formas de mitigar estas ameaças.
4. Deste modo, solicita-se a V.ª Ex.ª autorização para a realização de entrevistas aos seguintes elementos policiais da PSP, as quais poderão ser levadas a cabo de forma presencial ou via e-mail:

    - Exmo. Sr. Superintendente Domingos Antunes;
    - Exmo. Sr. Subintendente Francisco Alves;
    - Exmo. Sr. Subintendente Manuel Rodrigues.

5. Anexa-se o guião de entrevista.
6. A informação obtida contribuirá, de forma decisiva, para a redação de um capítulo da dissertação.
7. Mais se informa V.ª Ex.ª de que o Aspirante a Oficial de Polícia Mário Pereira se compromete a não usar os dados fora do âmbito deste trabalho académico.

O Diretor

José Carlos Bastos Leitão
Superintendente

R. 1º de Maio, nº3 1349-040 Lisboa Tel.: 213613900 Fax: 213610535 www.iscpsi.pt | iscpsi@psp.pt

147458
Página 1/1

Apêndice E – Tabela indicadores

Categorias	U.r.	Subcategorias	U.r.	Indicadores	U.r.
A	62	A.1	20	Impedir a desinformação	1
				Contrainformação	3
				Impacto negativo	1
				Disseminação de *Fake News*	11
				Determinar o impacto	4
		A.2	28	Manipular a realidade	23
				Capacidade de mobilização	5
		A.3	2	Escrutínio público	1
				Instabilidade	1
		A.4	12	Resposta oportuna	3
				Desmentir com o tempo	7
				Responder a *Fake News*	2
B	35	B.1	16	Recolher o máximo de informações	1
				Distinguir Informações	5
				Credbilizar a Informação	1
				Detetar informações falsas	5
				Gerir informações	4
		B.2	17	Disseminação de informação	3
				Partilha de informações falaciosas	2
				Disponibilidade de informação	3
				Liberdade de informação	4
				Sensibilização da sociedade	5
		B.3	2	Informações sensiveis	2

C	122	C.1	19	Falha na deteção de Fake News	2
				Manipular informação	3
				Gestão das informações	5
				Deteção de Fake News	2
				Fontes de Informação Policial	5
				Verificar a informação	1
				Gestão da desinformação	1
		C.2	19	Análise das informações	5
				Análise das Redes Sociais	13
				Análise da desinformação	1
		C.3	26	cenarização da informação	26
		C.4	58	Responder a Fake News	18
				Estratégia de comunicação	20
				Falta de Resposta eficaz	3
				Resposta eficaz à desinformação	13
				Resposta oportuna	4
D	53	D.1	22	Viralização das informações	10
				Viralização de fake News nas redes sociais	5
				Falta de ética	7
		D.2	11	Difrerenciação da perceção	5
				Perceber a importancia	5
				Dificuldade de determinar a veracidade da informação	1
		D.3	2	Confirmar a veracidade da informação	2
		D.4	18	Regular as redes sociais	6
				Falta de regulação	7
				Impacto das redes sociais	3
				Acesso às redes sociais	2

				Adaptar à realidade	13
				Fontes de informação	22
				Gestão ética	19
			E.1	82	Falta de ética	5
					Dever de Informação	3
					Partilha de informação pelos OCS	1
					Falta de Informação	3
					Análise das redes sociais	16
E	180				Dificuldade de verificação da informação	3
					Verificar a informação	43
			E.2	67	Partilha de informações falsas	10
					Partilha de informações credíveis	11
					Reagir à mentira	4
					Reagir pode levar a validação	1
			E.3	23	Reagir quando necessário	15
					Reagir a fake news	3
			E.4	8	Impacto dos orgãos de comunicação social	8