ACADEMIA MILITAR

CONTRIBUTO PARA UM MODELO DE MONITORIZAÇÃO POLICIAL DAS REDES SOCIAIS PELA GUARDA NACIONAL REPUBLICANA

Autor: Aspirante Aluno de Infantaria da GNR João Carlos de Almeida Canatário

Orientador: Professor Doutor José Fontes

Coorientador: Major de Infantaria da GNR Pedro Miguel Ferreira da Silva Nogueira

Mestrado em Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2018

ACADEMIA MILITAR

CONTRIBUTO PARA UM MODELO DE MONITORIZAÇÃO POLICIAL DAS REDES SOCIAIS PELA GUARDA NACIONAL REPUBLICANA

Autor: Aspirante Aluno de Infantaria da GNR João Carlos de Almeida Canatário

Orientador: Professor Doutor José Fontes

Coorientador: Major de Infantaria da GNR Pedro Miguel Ferreira da Silva Nogueira

Mestrado em Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2018

EPÍGRAFE

"Privacy is dead, and social media hold smoking gun"

Pete Cashmore (2009)

DEDICATÓRIA

Aos meus Avós,

que no fundo, sei que estiveram sempre comigo.

AGRADECIMENTOS

Manifesto a minha sentida gratidão e reconhecimento a todos os que tornaram a realização desta investigação possível.

Ao meu orientador, Sr. Professor Doutor José Fontes, a quem deixo uma palavra de profundo agradecimento pela permanente disponibilidade, suporte e constante colaboração que me prestou desde o planeamento até à conclusão da investigação.

Ao meu coorientador, Major de Infantaria da GNR, Pedro Miguel Ferreira da Silva Nogueira, pela prontidão que sempre manifestou, espírito critico, rigor e permanente disponibilidade.

Ao diretor dos cursos da GNR, Tenente-Coronel de Infantaria da GNR Nuno Alberto, pela constante ajuda e apoio, não só na realização da investigação, como também durante a frequência do tirocínio.

Ao Oficial de Ligação à *Guardia Civil,* Tenente-Coronel de Infantaria da GNR Mário Guedelha, pelo admirável trabalho desenvolvido, apoio e colaboração que permitiu ter um estágio de investigação aplicada bastante profícuo e importante.

Sincero agradecimento a todos os entrevistados pela disponibilidade e atenção concedida.

A todos os meus amigos e familiares que direta ou indiretamente me incentivaram e apoiaram ao longo desta caminhada.

Uma palavra de especial gratidão a todas as pessoas que corrigiram e acrescentaram valor a esta investigação.

Ao Curso Tenente-General Bernardim Freire de Andrade por todos os momentos que passamos juntos e nos fizeram únicos.

Ao XXIII curso de Oficiais da GNR, ao qual orgulhosamente pertenço e a quem sou grato por toda a amizade e camaradagem demonstrada ao longo deste percurso.

Ao meu Pai, pelos valores que sempre me ensinou e incutiu ao longo da vida, por me manter humilde na vitória e determinado no fracasso.

Com carinho, agradeço à minha Mãe, por toda a ternura, bem-querer, apoio, disponibilidade e amor incondicional.

Sem desprimor para os restantes familiares, queria agradecer ao Duarte pela lição de vida que sempre me ensinou, pois independentemente de tudo existe sempre lugar para um sorriso, um abraço e amor incondicional para dar.

De coração cheio, dedico uma palavra de amor à Ana, pelo carinho e compreensão demonstrada nos momentos de ausência e por continuamente me dar força e apoio para cumprir com o meu dever.

Por fim, quero deixar uma palavra de grande admiração ao Capitão de Infantaria Carlos Manuel de Almeida Canatário, meu irmão, pelas virgulas da diferença, pelo exemplo de dedicação e profissionalismo, por sempre me incutir um elevado espírito de dever e bem fazer, mas acima de tudo, por me dar a oportunidade única de poder privar e aprender com uma referência, respeitada e reconhecida, por subordinados, pares e superiores hierárquicos.

A todos um Bem-Haja,

João Canatário

RESUMO

As redes sociais são a força motriz da mudança do paradigma social que vivemos diariamente. Constituem-se como a principal via de comunicação e partilha de informação, o que tem levado a um aumento gradualmente acentuado da sua utilização. Através de uma análise cuidada da informação disponibilizada, é possível ter uma perceção daquilo que é a realidade social num contexto especifico, pelo que, urge monitorizar as redes sociais no âmbito policial.

A presente investigação, subordinada ao tema "Contributo para um Modelo de Monitorização das Redes Sociais pela Guarda Nacional Republicana", tem como objetivo geral compreender quais as características, capacidade e âmbito de atuação do modelo de monitorização policial das redes sociais por parte da Guarda Nacional Republicana. Para uma melhor orientação da investigação, foram definidos objetivos específicos, nomeadamente, caracterizar a monitorização nas redes sociais no âmbito da atividade policial, identificar o espetro de atuação da Guarda Nacional Republicana na monitorização das redes sociais, identificar as capacidades a desenvolver e as limitações a mitigar por parte da Guarda Nacional Republicana na monitorização das redes sociais e caracterizar a atuação da *Guardia Civil* na monitorização das redes sociais.

A metodologia empregue segue uma matriz dedutiva, com especial enfoque na análise da atuação da Guarda Nacional Republicana e *Guardia Civil* no âmbito da monitorização das redes sociais, visando, através de uma abordagem qualitativa, com recurso à analise bibliográfica e entrevistas, desenvolver uma cadeia de raciocínio em ordem descendente, de análise do geral para o particular, com vista a chegar a uma conclusão.

Concluímos que a informação obtida através da monitorização policial das redes sociais, quando associada a um determinado contexto social e/ou local e analisada por especialistas que entendem a realidade social, pode constituir-se como uma ferramenta preponderante na prevenção criminal, manutenção da ordem pública e paz social. No entanto, a Guarda Nacional Republicana ainda não desenvolveu esta potencialidade, pelo que o trabalho desenvolvido neste âmbito é diminuto e com fracos resultados operacionais. Para alterar esta situação é necessário definir os objetivos que se visa prosseguir com esta atividade, e consequentemente estabelecer uma *framework* organizacional. Só após esta

tarefa estar definida é que é possível capacitar a Guarda Nacional Republicana de meios técnicos e humanos.

Palavras-Chave: Guarda Nacional Republicana; Redes Sociais; Monitorização; Informações; Prevenção

ABSTRACT

Social networks are the driving force behind the change in the social paradigm we experiment on a daily basis. They constitute the prime way for the communication and information sharing, which has led to a gradually increasing of social media use. Through a careful analysis of the information available, it is possible to have a perception of what social reality is in a specific context, so it is urgent to monitor social networks in the police sphere.

The present research, under the theme "Contributo para um Modelo de Monitorização das Redes Sociais pela Guarda Nacional Republicana" has as general objective to understand the characteristics, capacity and scope of action of a police monitoring model of social networks by the Guarda Nacional Republicana. For a better orientation of the research, specific objectives have been defined, namely, to characterize monitoring in social networks within the scope of police activity, to identify the role played by the Guarda Nacional Republicana in monitoring social networks, identify the capacities to be developed and the limitations to be mitigated by the Guarda Nacional Republicana in the Monitoring of Social Networks and characterize the *Guardia Civil* role in monitoring social networks.

The methodology used follows a deductive matrix, with special focus on the analysis of the Guarda Nacional Republicana in and *Guardia Civil* in the scope of social network monitoring, aiming, through a qualitative approach, using bibliographical analysis and interviews, to develop a chain of reasoning in descending order of analysis from the general to the particular, to obtain a conclusion.

We conclude that the information obtained through police monitoring of social networks, when associated with a specific social and / or local context and analyzed by specialists who understand the "terrestrial reality", may constitute, as a preponderant tool in the criminal prevention and maintenance of public order and social peace. However, the Guarda Nacional Republicana is not awake for this potential, reason why, the work developed in this scope is small and with poor operational results. To change this situation, it is necessary to define the objectives to be pursued with this activity, and consequently establish an organizational framework. Only after this task is defined is it possible to equip the Guarda Nacional Republicana with technical and human means.

Key-Words: Guarda Nacional Republican; Social networks; Monitoring; Information; Prevention

ÍNDICE GERAL

ÍNDICE DE APÊNDICES E ANEXOS

ÍNDICE DE QUADROS

ÍNDICE DE FÍGURAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

A	
ANPC	Autoridade Nacional de Proteção Civil
APAV	Associação Portuguesa de Apoio à Vitima
AR	Assembleia da República
Art.º	Artigo
C	
CC	Convenção do Cibercrime
CERN	Conseil Européen pour la Recherche Nucléaire
Cfr.	Conforme
CGD	Caixa Geral de Depósitos
CI	Centro de Informações
CIDCP	Convenção Internacional dos Direitos Civis e Políticos
CO	Comando Operacional
CP	Código Penal
CPP	Código de Processo Penal
CTT	Correios de Portugal
D	
DCRP	Divisão de Comunicação e Relações Públicas
DGPJ	Direção Geral de Politica e Justiça
DI	Direção de Informações
DIC	Direção de Investigação Criminal
DLG	Direitos Liberdades e Garantias
DoD	Departemento da Defesa dos Estados Unidos da América
E	
EU	União Europeia
EUA	Estados Unidos da América

EUROPOL	*European Police Office*
F	
FRA	*Fundamental Rights Agency*
FS	Forças de Segurança
G	
GC	*Guardia Civil*
GCPGR	Gabinete Cibercrime da Procuradoria Geral da República
GNR	Guarda Nacional Republicana
I	
IA	Inteligência Artificial
IBM	Institute for Business Value
IoT	*Internet of Things*
ISP	Internet Service Providers
L	
LC	Lei do Cibercrime
LOGNR	Lei Orgânica da Guarda Nacional Republicana
LOIC	Lei da Organização da Investigação Criminal
LPDP	Lei de Proteção de Dados Pessoais
M	
MP	Ministério Público
O	
OE	Objetivo Específico
OPC	Órgão de Polícia Criminal
OSINT	*Open Source Intelligence*
P	
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
POI	Policiamento Orientado pelas Informações
Q	
QC	Questão Central
QD	Questão Derivada

R	
RASI	Relatório Anual de Segurança Interna
S	
SMS	*Social Media Services*
SOCMINT	*Social Media Intelligence*
T	
TIC	Tecnologias da Informação e Comunicação
TSI	Técnologias e Sistemas da Informação
U	
UCO	*Unidad Central Operativa*
UTPJ	*Unidad Técnica de Polícia Judicial*

INTRODUÇÃO

A sociedade atual é caracterizada essencialmente pela construção de um espaço de comunicação virtual à escala global, pois a crescente ubiquidade da informação, apoiada nas interações em tempo real, através da internet e da sua parte proeminente, a *World Wide Web* (WWW), contribui para uma contração do espaço pelo tempo (Castells, 1996). Esta omnipresença da informação moldou todo o contexto social, levando à emergência da sociedade da informação, onde as Tecnologias de Informação e Comunicação (TIC), aliadas a dispositivos móveis, permitem assegurar o acesso permanente aos recursos informativos.

A facilidade de acesso à informação, introduzida pela natural evolução da tecnologia, veio impreterivelmente redirecionar muita da atividade humana do espaço físico para o ciberespaço. Nesta migração estão incluídos processos de comunicação e de interação social, facilitados essencialmente por serviços de *social media*, nos quais se incluem as redes sociais.

Este novo paradigma da realidade social é enfatizado pelo crescente número de utilizadores da internet e das redes sociais, estando sempre numa tendência de crescimento[1]. Esta dimensão da vida social exige, tal como no espaço físico, a atuação das Forças e Serviços de Segurança (FSS) numa perspetiva de garantir a segurança tanto dos cidadãos, como da própria estrutura tecnológica, cada vez mais essencial num mundo globalizado.

A internet enquanto elemento essencial da conexão global de aproximação cultural, social e económica, revela-se como um elemento catalisador do cibercrime e da criminalidade tecnológica. Esta tipologia de crime é potenciada por vários elementos, como a inexistência de fronteiras no ciberespaço[2] e a evolução exponencial da tecnologia, que permite aumentar a capacidade de anonimato dos seus atores, bem como o aumento da complexidade dos crimes perpetrados.

[1] De Acordo com dados de da plataforma *We are Social.*

[2] O que põem desde logo em causa o princípio da territorialidade, amplamente aplicado nos crimes perpetrados no espaço físico, exigindo assim um esforço tremendo de cooperação e partilha de informação entre autoridades judiciárias, *Internet Service Providers*(ISP), e Serviços de *Social Media* (SMS), que se regem muitas vezes por ordenamentos jurídicos distintos, o que dificulta a recolha de prova digital.

Esta realidade social e criminal não tem efeitos apenas no ciberespaço, pois todos os desenvolvimentos nas TIC facilitam a atividade criminosa no espaço físico. Este facto, aliado à prova digital, despoletou problemas específicos em matéria processual penal, que obrigam a repensar conceitos e problemas jurídicos já consolidados na sua atuação no mundo físico (Ramalho, 2017).

Segundo Quivy e Campenhoudt (2013) "a escolha de uma problemática não depende (...) do acaso ou da simples inspiração pessoal do investigador. Ele próprio faz parte de uma época (...) os seus acontecimentos marcantes", já a justificação do tema está diretamente ligada ao seu carácter inovador e atual (Sarmento, 2013).

A escolha do tema surge da intrínseca curiosidade do autor pela tecnologia informática, pelo facto de ter sido estudante de engenharia informática na Universidade de Aveiro (UA) e pela crença de que as redes sociais são o principal modelador da sociedade atual.

A escolha do tema deve-se também à maneira como as redes sociais criaram novas formas de interação e partilha da informação. Estas características fizeram destas plataformas meios de rápida disseminação de dados, noticiais, transmissão em tempo real de eventos sociais e, portanto, tornaram-se num meio de escrutínio permanente de qualquer atividade humana, seja ela individual ou coletiva. Vieram também facilitar a mobilização para comportamentos coletivos como manifestações e protestos, tanto em ambiente digital como no espaço físico (Preece et al., 2018). É neste contexto que surge o interesse das Forças e Serviços de Segurança na monitorização das redes sociais, pois a informação está em grande parte disponível para ser recolhida, tratada e analisad, sendo então produzidas informações policiais, que servem como uma ferramenta de compreensão situacional, bem como de apoio à decisão. Este tipo de informações impulsiona a previsão de perigos através de um policiamento preditivo que contribui para a superintendência da ordem pública (Moleirinho, 2009).

A monitorização das redes sociais está de facto na ordem do dia, o que enfatiza pertinência do seu estudo. Já em 2018 surgiram notícias acerca de dados de milhões de utilizadores da rede social *Facebook* terem sido indevidamente utilizados para manipular opiniões relativamente às eleições Presidenciais dos Estados Unidos da América (EUA). Uma das grandes mudanças sociais e políticas da última década, a primavera árabe, teve por base o levantamento e reunião de manifestantes nas redes sociais. Distúrbios civis em

cidades inglesas e canadianas[3] enfatizaram o uso do *Twitter*, *Facebook* & *Youtube* como instrumentos de coordenação, preparação e propaganda dos manifestantes. Também no âmbito criminal, a criminalidade informática em Portugal registou 976 casos apenas no ano de 2017, o que corresponde a um aumento de 326% em relação à primeira medição efetuada em 2006, confirmando assim uma tendência de crescimento ano após ano.[4]

Na esfera nacional, o conceito estratégico de segurança interna estabelece como linha de ação estratégica "o alargamento do sentimento de segurança à dimensão do ciberespaço" (Lourenço, Lopes, Rodrigues, Costa, & Silvério, 2015, p. 55). No âmbito institucional, a Estratégia da Guarda 2020 define como um dos desafios da instituição "assegurar a presença e atuação progressiva no mundo ciber, afirmando a Guarda como determinante no mundo real e no mundo virtual" (Guarda Nacional Republicana [GNR], 2014).

É então, perante esta problemática de monitorização das redes sociais, que surge este Relatório Científico Final do Trabalho de Investigação Científica (RCFTIA), subordinado ao tema: "Contributo para o Modelo de Monitorização Policial das Redes Sociais pela Guarda Nacional Republicana".

A apresentação de um Trabalho de Investigação Aplicada (TIA) é parte integrante da estrutura curricular do ciclo de estudos do Mestrado Integrados em Ciências Militares na especialidade de Segurança da Guarda Nacional Republicana (GNR), sendo apresentado no quinto e último ano de frequência na Academia Militar (AM)

Sendo a monitorização das redes sociais o cerne da investigação, foi definido o objetivo geral de compreender quais as características, capacidades e âmbito de atuação de um modelo de monitorização policial das redes sociais por parte da GNR. Com vista a dotar o referido objetivo de um carácter mais concreto e abrangente, foram definidos quatro objetivos específicos (OE), tendo cada um deles uma função intermediária e instrumental, o que possibilita concretizar o objetivo geral e uma melhor orientação da investigação (Marconi & Lakatos, 2003).

Os objetivos específicos formulados são os seguintes:

OE1: Caracterizar a Monitorização nas Redes Sociais no âmbito da atividade Policial.

OE2: Identificar o espetro de atuação da GNR na Monitorização das Redes Sociais.

[3] Londres em 2012 e Vancouver em 2011.

[4] Segundo dados do Relatório Anual de Segurança Interna de 2017.

OE3: Identificar as capacidades a desenvolver e as limitações a mitigar por parte da GNR na Monitorização das Redes Sociais.

OE4: Caracterizar a atuação da *Guardia Civil* na Monitorização das Redes Sociais.

O quarto objetivo específico surge como forma de observar e caracterizar um modelo de monitorização policial das redes sociais, numa realidade social parecida à portuguesa, que derivado a algumas variantes políticas e históricas, tem experienciado alguma consternação social com as redes sociais a desempenharem um papel fundamental. O facto da *Guardia Civil* ser uma congénere da GNR e também uma força de segurança de natureza militar, enfatiza a relevância e pertinência deste eixo de aproximação.

Considerando o objetivo geral, formulou-se a questão central. Segundo Fortin (2000), deve ser uma interrogação explicita, com o objetivo de obter novas informações sobre um domínio que deve ser explorado. Desta forma, a questão central desta investigação é: "Que modelo de monitorização policial das redes sociais deve ser desenvolvido pela GNR?"

A investigação está dividida em três capítulos fundamentais. Após a introdução do trabalho surge o enquadramento teórico, resultante da revisão bibliográfica. No Capítulo I são dados a conhecer os conceitos, perspetivas teóricas e pesquisa empírica de referência com particular relevância para a investigação em causa, com particular incidência para a evolução da internet, monitorização das redes sociais e *Social Media Intelligence* (SOCMINT), bem como no domínio da segurança, globalização informações policias, discurso de ódio e cibercrime.

O segundo capítulo está subordinado ao enquadramento metodológico quanto ao tipo de abordagem, modelo de investigação, modelo de análise de resultados e apresentação da questão central e as questões derivadas. É também neste capítulo que são especificados, com base no contexto de observação, os métodos e técnicas de recolha, tratamento e análise de informação.

No terceiro capítulo é apresentada a análise e discussão dos resultados, decorrente do trabalho de campo efetuado pelo investigador.

Por fim são apresentadas as conclusões da investigação e feitas as recomendações para investigações futuras.

CAPÍTULO 1
ENQUADRAMENTO TEÓRICO

1.1. Definição e Evolução do Conceito de Segurança

A segurança personificada na "preservação do indivíduo e da sua propriedade é uma das atividades do Homem tão antiga quanto o próprio conceito de propriedade permite" (Cruz, 2015, p. 91).

Segurança é um termo polissémico. Ou seja, o seu significado varia consoante de acordo com o contexto a que se reporta, resultado de uma realidade complexa e abrangente, ainda que seja desejável estabelecer critérios que possam objetivar a noção de segurança (Cruz, 2015).

Segurança pode ser vista segundo duas abordagens distintas. A abordagem politologia, que classifica segurança com um dos fins do Estado, sendo que a abordagem sociológica a classifica como uma função, conjunto de atividades e tarefas especializadas. Em consequência destas duas abordagens, existe uma diferenciação entre os variados autores que se dedicam a esta temática. Enquanto uns definem segurança como um estado ou condição, seja ela de natureza física, psicológica ou social, outros referem-se a esta como um conjunto de medidas (Alves, 2010).

O mesmo autor define segurança, como *"*a condição que se estabelece num determinado ambiente, através da utilização de medidas adequadas, com vista à sua preservação e à conduta de atividades, no seu interior ou em seu proveito, sem ruturas*"* (Alves, 2010, p. 37).

De uma forma mais simplificada, segurança pode ser encarada como "o estado de tranquilidade resultante da ausência de perigo, ou pelo menos, da perceção real de risco" (Clemente , Polícia e Segurança, 2010, p. 155).

Em consonância com a definição de segurança como condição, estabelece-se como objeto da segurança a realidade que se "oferece à vista e que ocupa o espírito, afigura-se, pois, a resposta adequada afirmar que sempre será um dado ambiente, compreendido nele o seu conteúdo, com diversos componentes em interação e centrado na pessoa humana enquanto sua principal beneficiária" (Alves, 2010, p. 38).

A segurança é o resultado de "um produto do sistema social, refletindo, por isso, de forma continuada, as condições estruturais e conjunturais de um sistema assaz complexo, onde interagem questões tão diversas como a educação familiar, o nível escolar, a saúde física e mental ou o emprego" (Viegas, 1998, p. 190).

1.1.1 Globalização e Sociedade da Informação

No seu senso comum a palavra "globalização" refere-se ao alargamento, aprofundamento e aceleração da interligação global, sendo a "força central por trás das rápidas mudanças sociais, politicas e económicas que estão a remodelar as sociedades modernas e a ordem mundial" (Held, McGrew, Goldblatt, & Perraton, 1999, p. 16).

O conceito de globalização implica um prolongamento dos efeitos da atividade social, económica e política para além das fronteiras (de qualquer índole), pelo que, eventos, decisões e atividades numa região do globo podem ter uma importância significativa para indivíduos ou comunidades numa outra região distante do globo (Held et al., 1999).

Waters (1999) defende que a globalização é um processo social através do qual se diminuem os constrangimentos geográficos sobre os processos sociais e culturais, sendo que a consciencialização individual dessa redução é cada vez mais abrangente. Mesmo sendo um processo social, a globalização não possui nenhum mecanismo de controlo ou de abrandamento, pois "é um fenómeno cada vez mais descentralizado, que não está sob o controlo de nenhum grupo de nações e ainda menos sob o domínio das grandes companhias" (Giddens, 1999, p. 27).

A globalização tem um aspeto inegavelmente material, na medida em que é possível identificar por exemplo fluxos comerciais, de capitais e de pessoas em todo o mundo (Giddens, 1999).

Segundo Castells (1996), as estruturas em rede não são uma novidade da sociedade da informação, no entanto, as tecnologias e sistemas de informação impulsionados pela internet têm vindo a alterar os processos sociais. O mesmo autor refere que as redes, historicamente, existiam numa base física material, no entanto, "a sociedade em rede difunde-se seletivamente por todo o planeta, trabalhando em *sites*, organizações e instituições, constituindo assim a maior parte do ambiente material da vida das pessoas" (Castells, 1996, p. 43).

1.2. Dimensão Ciber

1.2.1 Ciberespaço

Para analisar o cibercrime e a monitorização policial das redes sociais é condição *sine qua non* estabelecer o conceito de ciberespaço, pois é neste que se desenvolve toda a atividade de âmbito digital. O conceito de ciberespaço é altamente mutável, evoluindo em função daquilo que são os avanços das Tecnologias e Sistemas de Informação (TSI), e por isso torna-se extremamente difícil de definir. Em virtude desta dificuldade, o ciberespaço acaba por ser muitas vezes associado à internet, o que não podia ser mais errado. É então importante diferenciar, pois a internet e ciberespaço, apesar de estarem relacionados, não têm o mesmo significado, uma vez que, "o ciberespaço diz respeito à dimensão digital daquilo que fazemos enquanto a internet é constituída por uma rede física de computadores (o *hardware*) (Betz & Stevens, 2012, p. 13).

A dificuldade em definir aquilo que é o ciberespaço é espelhado pelas doze definições já divulgadas pelo Pentágono, sendo a última "o domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computadores e os seus processadores e controladores" (Singer & Friedman, 2014, p. 13). Singer e Friedman (2014, p.13), apesar de corroborarem com a definição apresentada, acabam por apresentar uma versão simplificada, pois "na sua essência, o ciberespaço é o domínio de redes de computadores (e os usuários por trás dele), em que a informação é armazenada, partilhada e comunicada online".

Já tendo sido referida a diferença entre internet e o ciberespaço, importa também distinguir, em virtude da definição apresentada, computador de ciberespaço. Na verdade, o ciberespaço surge muito antes da invenção do computador. Se considerarmos o telefone e a televisão como um meio de comunicação e partilha da informação, torna-se intuitivo perceber a diferença entre ciberespaço e computador. A introdução da *Internet of things* (IoT) vem realçar a abrangência do ciberespaço a todos os aparelhos com capacidade de processamento (Barrinha & Carrapiço, 2016).

Neste sentido uma definição mais abrangente é exigida, pelo que a *Intermational Telecomunication Union* (ITU), define ciberespaço como o conjunto de "utilizadores, redes, dispositivos, *software*, processos, informações em armazenamento ou trânsito,

aplicações, serviços e sistemas que podem ser conectados direta ou indiretamente a redes" (Internation Telecommunication Union [ITU], 2009, p. 27).

Uma das características do ciberespaço prende-se com o aumento estonteante da frequência e velocidade das comunicações, pelo que a distância comunicacional entre indivíduos, instituições e até mesmo os Estados, foi drasticamente reduzida, tornando-se em alguns casos irrisória (Strate, 1999).

Em consequência desta característica surge um problema de delimitação, pois ao contrário do espaço físico, as fronteiras são inexistentes. Este facto dificulta qualquer poder estatal de exercer a sua soberania (Strate, 1999).

A falta de delimitação para o exercício da soberania enfatiza uma outra problemática: a da aplicação da Lei perante factos ilícitos praticados. A facilidade com que se podem realizar ações no ciberespaço sob anonimato vem adensar ainda mais a referida problemática (Strate, 1999).

Em resultado das várias características elencadas, com especial enfoque para o anonimato, mobilidade e anarquia do ciberespaço, foi criado um ambiente criminal altamente complexo e difícil de combater, o que torna a missão das FSS no ciberespaço bastante difícil (Kozlovski, 2007).

1.2.2 Cibersegurança

O conceito de cibersegurança surge da necessidade intrínseca de segurança em todos os domínios da atividade humana, pois "num mundo globalizado, um dos desafios que mais prementemente se colocam aos Estados é o da segurança, sendo a vertente da cibersegurança incontornável num mundo cada vez mais dependente do eficaz funcionamento de sistemas informáticos" (Verdelho, 2005, p. 159). No entanto, em consequência das características ímpares do ciberespaço, a definição de segurança aplicada aos domínios físicos[5] não pode ser adotada ao domínio do ciberespaço. Desta forma, torna-se extremamente difícil ter uma noção holística daquilo que é a cibersegurança.

A *Karspersky*[6] define cibersegurança como "a prática de defender computadores, servidores, dispositivos móveis, sistemas eletrónicos, redes de comunicação e dados de ataques maliciosos ou acessos não autorizados" (Kaspersky Laboratories, 2018, p. 1). De

[5] Terra, ar, água e Espaço.
[6] Empresa líder Mundial no desenvolvimento de software anti-virus.

uma forma lógica pode entende-se como "(...) todas as dimensões de segurança que afetam o ciberespaço (...)" (Caldas, 2011, p. 2).

Essencialmente, "as questões/soluções de cibersegurança devem ter o seu ponto de partida no valor da informação, mais do que nos aspetos tecnológicos que, embora sendo de tratamento obrigatório e não dispensáveis, são subsequentes" (Caldas & Freire, Cibersegurança: das Preocupações à Ação, 2013, p. 2).

Assim o problema que se pretende mitigar com a cibersegurança é garantir a segurança da informação dos cidadãos, das organizações e do Estado, que é armazenada e comunicada através das Tecnologias da Informação e Comunicação (TIC). A Informação e toda a estrutura que a suporta, asseguram o normal funcionamento das infraestruturas críticas[7] essenciais à vida em sociedade, tal como a conhecemos hoje (Santos, 2014).

Portugal, tal como a grande maioria dos Estados-Membros da União Europeia (UE), optou por um modelo interdepartamental de resposta à cibersegurança, ou seja, as competências e responsabilidades atribuídas a cada setor ou entidade governamental no mundo físico são transpostas para o ciberespaço. Desta forma, cabe às autoridades judiciárias e de polícia a prevenção, combate e investigação criminal relativos ao cibercrime (Robinson, Gribbon, Horvath, & Robertsion, 2003).

1.2.3 Cibercrime

O conceito de cibercrime é hoje pouco exato e abrangente e, por conseguinte, pouco unânime entre a comunidade jurídica. As características do referido conceito, em muito se devem ao ritmo estonteante da evolução das TSI[8], característica do ciberespaço (por si só abstrato) e ao elevado espectro de tipologias que pode assumir (Ghosh & Turrini, 2010).

Se considerarmos este conceito num sentido amplo, podemos abranger:

> "toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que esses não sejam mais que um instrumento para a sua prática, mas que não integram o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios" (Venâncio, 2011, p. 16).

Esta posição é corroborada por Marques & Martins (2006, p. 29) ao considerarem cibercrime como "todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou, em que o computador é alvo simbólico desse ato ou que o computador é objeto de crime."

[7] Sistema bancário e de telecomunicações, bem como, o de abastecimento de água eletricidade e serviços de emergência.

[8] Propicio a uma desatualização dos conceitos jurídicos e adaptação dos meios de investigação criminal.

Por outro lado, temos o conceito em sentido restrito, onde cibercrime engloba crimes em que o meio informático surge como parte integradora do tipo legal ou do seu objeto de proteção, ainda que o bem jurídico protegido não seja digital (Rodrigues, 2009).

A Comissão Europeia subdivide o cibercrime em três categorias distintas: as formas tradicionais de criminalidade cometidas através das TSI[9]; os crimes relacionados com a publicação e divulgação de conteúdo ilícito[10] através do recurso às TSI em redes de comunicação eletrónicas; crimes exclusivos das redes eletrónicas ou crimes informáticos em sentido estrito[11], ou seja, ataques contra as TSI (Conselho Europeu [CE], 2001).

Já a doutrina portuguesa vai mais longe, ao admitir mais uma categoria de atividade criminosa associada ao cibercrime, neste caso, os crimes relativos à proteção de dados pessoais ou da privacidade[12] (Ascensão, 2001).

A referida doutrina acaba por catalogar e especificar alguns crimes nas categorias anteriormente mencionadas. No que concerne às tipologias tradicionais de crime cometidos através das TSI, entende-se que não existe uma alteração do tipo penal comum, correspondendo a utilização destas tecnologias a uma especificação ou qualificação do crime, como é exemplo o crime de burla informática e das comunicações[13]. Dos crimes relacionados com a publicação e divulgação do conteúdo, perpetrados por meios de comunicação eletrónicos, destaca-se a difusão de pornografia infantil[14] e a discriminação racial ou religiosa[15]. Os crimes relativos à proteção de dados pessoais ou da privacidade estão explanados em Lei própria[16]. Por fim, os crimes informáticos em sentido estrito ou exclusivos das redes eletrónicos[17], nos quais o meio informático é o elemento próprio do tipo de crime estão previstos pela Lei do Cibercrime (LC)[18].

[9] Cfr. art.º 7º e 8º da Convenção do Cibercrime.
[10] Cfr. art.º 9º da Convenção do Cibercrime.
[11] Cfr. art.º 2º a 6º da Convenção do Cibercrime.
[12] Decorrente da Lei 67/98, de 26 de outubro, da transposição da Diretiva 95/46/CE e da Lei 69/98, de 28 de outubro. Em breve (25 de maio de 2018) revogada pela nova Lei de Proteção de Dados Pessoais.
[13] Cfr. art.º 221º do Código Penal.
[14] Cfr. alínea d) nº3 do art.º 172º do Código Penal.
[15] Cfr. alínea a) nº1 do art.º 240º do Código Penal.
[16] Cfr. art.º 43º a 47º da Lei 67/98.
[17] Cfr denominação atribuída pela Comissão Europeia.
[18] Lei 109/2009 de 15 de setembro.

1.2.4 Convenção e Lei do Cibercrime

A Convenção do Cibercrime (CC)[19] foi o culminar de um conjunto de iniciativas diplomáticas e jurídicas desenvolvidas pela União Europeia (UE), face à crescente preocupação por esta temática, tendo em vista a criação de instrumentos legislativos que se adequem a realidade jurídica à evolução estonteante das TSI. A convenção teve três objetivos centrais:

> "Em primeiro lugar, criar um conjunto de infrações comuns entre os Estados signatários; em segundo lugar, criar um conjunto de medidas processuais que permitam às autoridades competentes de cada Estado recolher prova em ambiente digital no seu território; e por último, estabelecer mecanismos de cooperação internacional que facilitem a recolha, conservação e transmissão rápida e eficaz de prova localizada em Estados diversos daquele no qual decorre o procedimento criminal" (Ramalho, 2017, p. 69).

É através da resolução da Assembleia da República (AR) nº 88/2009 e do Decreto do Presidente da República nº 92/2009, publicados em 15 de setembro, que Portugal acaba por retificar a CC. Em virtude da referida retificação da Decisão-Quadro 2005/222/JAI,[20] bem como a ineficácia e desatualização do Código Penal (CP) e da Lei da Criminalidade Informática[21] aliada aos avanços tecnológicos do cibercrime, levou ao surgimento da LC (Simas, 2014).

A LC passa a integrar num único diploma legal todas as normas respeitantes ao cibercrime, incluindo normas de Direito Penal Material, através da criação de novas tipologias de crime e disposições relativas à relevante cooperação[22] internacional (Assembleia da República [AR], 2009).

No que refere às disposições penais materiais, apesar de excluir o catálogo de crimes do CP referentes a esta temática, a LC acaba por englobar[23] nos artigos 3º a 8º, os crimes de Falsidade Informática; Dano Relativo a Programa ou outros Dados Informáticos; Sabotagem Informática; Acesso Ilegítimo; Interceção Ilegítima, e Reprodução Ilegítima de Programa Protegido, respetivamente. Todo este catálogo é referente à categoria dos crimes informáticos em sentido restrito, nos quais o meio informático é o elemento próprio do tipo de crime (AR, 2009).

---

[19] Adotada em Budapeste a 23 de novembro de 2001.
[20] Relativa a ataques contra sistemas de informação.
[21] Lei 109/1991 de 17 de agosto.
[22] Ponto de contato 24/7 na dependência da PJ, cfr. art.º 21º da Lei do Cibercrime.
[23] Em conformidade com os crimes presentes na Convenção do Cibercrime.

No capitulo III surgem as disposições processuais e as medidas processuais penais para a recolha da prova digital, estando previstas entre os artigos 12º e 19º, sendo respetivamente a Preservação expedita de dados de tráfego; a Revelação expedita de dados de tráfego; Injunção para apresentação ou concessão do acesso a dados; Pesquisa de dados informáticos; Apreensão de dados informáticos; Apreensão de correio eletrónico e registos de comunicações de natureza semelhante; Interceção de comunicações; e Ações encobertas (AR, 2009).

Não sendo o objetivo desta investigação fazer uma análise jurídica destas disposições processuais, importa referir que, as mesmas se devem essencialmente à possibilidade [24] de preservação [25], pesquisa [26] e acesso de dados informáticos [27] e de tráfego [28], bem como a apreensão de correspondência eletrónica e/ou registos de comunicações [29] e interceção [30] das mesmas. É ainda permitido o recurso a ações encobertas[31], nos termos previstos na Lei 101/2001, de 25 de agosto.

Todo este catálogo de medidas processuais deve ser "analisado como um todo, pois em muitos aspetos práticos relacionam e complementam-se" (Venâncio, 2011, p. 67). Esta complementaridade veio enfatizar a problemática referente à conservação de dados pelos *Internet Service Providers* (ISP), pois este setor tem vindo a ser "afetado pela desregulamentação, pela abertura à concorrência e pelas privatizações, a que acrescem os agrupamentos de vocação mundial que se vão constituindo entre os seus operadores" (Militão, 2013, p. 268). Este paradigma tem levado a uma privatização da investigação, sendo confiadas a este setor tarefas de "intromissão, interceção e gravação de telecomunicações e, em geral, da produção e armazenamento de dados processualmente relevantes, bem como a sua apresentação ao processo penal" (Militão, 2013, p. 269).

A problemática estende-se aos provedores de serviço de correio eletrónico e de *Social Media.* Perante estes factos, o Gabinete de Cibercrime da Procuradoria-Geral da República (GCPGR), encetou contatos com os vários operadores, nomeadamente a *Microsoft*, a *Google* e o *Facebook*, com o propósito de estabelecer critérios de entendimento e cooperação. "Em resultado dessa abordagem, passou a ser possível

[24] Mediante autorização judiciária
[25] Cfr. art. º 12º e da LC.
[26] Cfr. art. º 14º da LC
[27] Cfr. alínea b) do art.º 2º da LC.
[28] Cfr. alínea c) do art.º 2º da LC.
[29] Cfr. art. º 17º da LC
[30] Cfr. alínea d) do art.º 2º e 18º da LC.
[31] Apenas nos casos previstos no nº1 do art.º 19º da LC.

formular diretamente pedidos àqueles fornecedores de serviços norte-americanos, sem necessidade de recurso aos canais da cooperação internacional" (Procuradoria-Geral da República [PGR], 2017).

1.2.5 Competências da GNR no Cibercrime

A prevenção "é o objetivo principal da função polícia (...) [sendo conseguida] com base em informações, isto é, conhecimento (...) das ameaças que permitam prever acontecimentos- através de presença, de vigilância e atividades (...)" (Alves, 2008, p. 134). Assim sendo, a primeira forma de atuação da GNR neste âmbito é através da prevenção, pois:

> "constitui a melhor forma de detetar, evitar e lutar contra os efeitos do cibercrime, incrementando a literacia informática. A prevenção será alcançada com informação, sensibilização e preparação, através de seminários, campanhas visadas a um público-alvo comum ou específico, alertando para os riscos e perigos do mundo cibernético e os meios de proteção e responsabilidade de utilização" (Rodrigues, 2009, p. 78).

No âmbito da investigação, a GNR, enquanto Órgão de Polícia Criminal (OPC)[32] de competência genérica, "desenvolve um conjunto de ações que visam prevenir a criminalidade em geral e efetuar diligências necessárias tendentes a investigar a existência de um crime e proceder à recolha de prova, determinar os seus agentes, a sua responsabilidade e efetuar as consequentes detenções[33]" (Branco, 2010).

A GNR tem competência genérica na investigação de crimes cuja competência não esteja reservada noutros OPC, ou que a investigação lhe seja cometida pela autoridade judiciária[34]. Ainda que os "crimes informáticos e praticados com recurso a tecnologia informática[35]" (Assembleia da República [AR], 2008) sejam da competência reservada da PJ, podem ser deferidos noutros OPC.

Neste âmbito, importa referir que cabe ao Ministério Público (MP) dirigir o inquérito[36], podendo delegar em qualquer OPC competências de investigação, mesmo que o crime em questão seja da competência reservada[37] da PJ.

---

[32] Cfr. alínea b) nº1 do art.º 12º da LOGNR.
[33] Cfr. alínea a) e b) nº4 do art.º 3º da LOIC.
[34] Nos termos do art.º 8º da LOIC
[35] Cfr. alínea l) nº3 do art.º 7º da LOIC.
[36] Cfr. art.º 262 do CPP.
[37] Ver Acórdão 50/14.0SLLSB-Y.L1 - 9 do Tribunal da Relação de Lisboa.

Não obstante, e cumprindo as disposições revistas na LOIC, no que se refere às competências de cada OPC em matéria de investigação criminal, os crimes previstos no nº3 do art.º 7, "crimes informáticos e praticados com recurso a tecnologia informática"[38] (AR, 2008), apesar de serem da competência reservada da PJ, podem ser delegados noutro OPC, nos termos do art.º 8º da LOIC.

Assim, sempre que "tal se afigure, em concreto, mais adequado ao bom andamento da investigação" (AR, 2008), pode ser delegada na GNR a investigação de um crime praticado com recurso a tecnologia informática, com particular enfoque para quando se trata de "crime sobre o qual incidam orientações sobre pequena criminalidade, nos termos da Lei de Politica Criminal em vigor (...)" (AR, 2008).

A LC estabelece[39] que as disposições processuais previstas no seu Capítulo III "aplicam-se a processos relativos a crimes: a) Previstos na presente lei; b) Cometidas por meio de um sistema informático; ou c) Em relação aos quais seja necessário proceder à recolha de prova em suporte informático" (AR, 2009).

O previsto na alínea b) e c) do nº1 do art.º 11º da LC pressupõe um alargamento do âmbito de aplicação, desde logo a todas as categorias de cibercrime anteriormente descritas, bem como aos crimes em que, decorrente da investigação, exista a necessidade de recolha de prova digital. Assim sendo, a GNR pode e deve utilizar as medidas processuais previstas na LC (descritas no subcapítulo anterior) nas investigações em que se afigure necessário tomar medidas cautelares e de polícia referentes à prova digital. (AR, 2009).

1.3. Internet e Redes sociais

"A internet representa um dos mais bem-sucedidos exemplos dos benefícios do investimento sustentado e do compromisso com a pesquisa e desenvolvimento da infraestrutura da informação" (Clark et al., 1997, p. 2).

A internet surgiu em 1968 através de um protocolo formalizado entre a Agência de Projetos de Pesquisa Avançada do Departamento de Defesa (DoD) dos EUA e o *Institute for Business Value* (IBM), denominado de *Advanced Research Project Agency Net* (ARPANet). Esta tecnologia tinha por objetivo interligar as bases militares e o DoD, bem

[38] Cfr. alínea l) nº3 do art.º 7º da LOIC.
[39] Cfr. alínea nº1 do art.º 11º da LC.

como estabelecer-se como um sistema de comunicação em caso de ataque nuclear[40] (Clark , et al., 1997).

O conceito de "interneting"[41] surgiu quando a ARPANet evoluiu para a rede de internet. Esta rede tinha como conceito central a existência de várias redes independentes integradas umas nas outras, começando com a ARPANet como a rede pioneira de comutação de pacotes[42], mas que rapidamente integrou pacotes de redes de satélites, bem como pacotes de rede de rádios de base terrestre. Desta forma, a internet, tal como a conhecemos hoje, incorpora subjacentemente a ideia chave de uma arquitetura aberta de rede (Clark et al., 1997).

Ao integrar várias redes numa só, era necessário criar um conjunto de regras[43] e procedimentos, de modo a existir uma sincronização entre todos os seus intervenientes. Perante esta necessidade é implementado no início da década de 1970 o protocolo TCP/IP. Esta sigla é resultante da junção do *Transmission Internet Protocol* (TCP) e o *Internet Protocol* (IP). Este protocolo especifica como os dados são trocados pela internet, fornecendo comunicações *peer-to-peer* que identificam como devem ser divididos em pacotes, endereçados, transmitidos, encaminhados e recebidos no destinatário. O principal objetivo do TCP/IP foi contruir uma interconexão entre as diversas redes que constituem a internet, fornecendo serviços de comunicação universal entre todas elas, incluindo as redes físicas. O benefício deste protocolo foi permitir a comunicação entre utilizadores/anfitriões em diferentes redes, mesmo que separados por uma grande área geográfica (Parzlale, et al., 2006).

Com todos os avanços tecnológicos a ARPANet começou a expandir-se até a um ponto de rutura que levou à sua extinção, originando assim duas redes distintas; a *Military Network*, unicamente relacionado a assuntos militares; e a internet de âmbito público. A internet continuou confinada exclusivamente às universidades, o que viria a mudar com a difusão massiva dos computadores pessoais, permitindo um avanço para o domínio pessoal e global (Giddens & Sutton, 2013).

A *World Wide Web* (WWW), comumente conhecida como a web, não é um sinónimo de internet, mas é sem duvida a sua parte mais proeminente, podendo ser

[40] Em 1968 os EUA estavam em plena Guerra Fria.

[41] Fazer uso da internet ou a procura pela informação.

[42] Em informática o significado da palavra "pacote" reporta-se a uma estrutura unitário de transmissão de dados e/ou uma sequência de dados transmitidos por uma rede ou linha de comunicação que utilize a comutação de pacotes.

[43] Tal como uma Língua em que todos os intervenientes percebem o significado e sentido de cada palavra.

definida como um sistema tecnológico-social, com o objetivo de interagir com os seres humanos, tendo por base as redes tecnológicas. Um sistema tecnológico-social é aquele que enfatiza a correlação entre a cognição e a comunicação (Aghaei, Nematbakhsh, & Farsan , 2012).

Hoje a tecnologia Web pode ser facilmente definida por cada utilizador de uma maneira diferente e arbitrária, mas tendo sempre por base um sistema interconectado de documentos *hypertext* que podem ser acedidos via internet. Esta tecnologia foi introduzida Tim Burners-Lee[44] no ano de 1989. Inicialmente tinha como objetivo melhorar a eficiência das comunicações do *Conseil Européen pour la Recherche Nucléaire* (CERN), mas rapidamente o seu inventor se apercebeu do seu potencial global. É então em 1990, num trabalho conjunto entre o seu inventor e o cientista computacional Robert Cailliau, que é proposta a utilização de *hypertext* para ligar e acessar informações de vários tipos como numa rede de nós, na qual, o utilizador pode navegar e explorar à sua vontade (Berners-Lee & Cailliau, 1990).

Desde a sua génese (Web 1.0) a web já vai na sua terceira geração, tendo evoluído para Web 2.0 e posteriormente para Web 3.0.

A Web 1.0 considerada pelo seu criador como *read-only*[45], ou comumente conhecida como Web documental é definida como "um espaço de informação, no qual os tópicos de interesse referidos como recursos são identificados por um identificador universal denomiando *Uniform Resources Identifiers* (URL)" (Choudhury, 2014, p. 22). Esta primeira geração era classificada como passiva e estática, o que de certa forma é percetível dado o seu fluxo unidirecional. Composta maioritariamente por páginas estáticas, tendo como único propósito e divulgação de conteúdo, esta geração era bastante limitada no que concerne à interação e contribuição de conteúdos entre os utilizadores e a página em si (Aghaei et al., 2012).

A partir de 2004 esta dinâmica entre o utilizador e os conteúdos disponíveis nas páginas da internet viria a mudar drasticamente com a introdução da segunda geração da WWW, a Web 2.0. Foi denominada por Tim O'Reilly (2005), um dos seus principais impulsionadores, como a *Read-Write Web*, *Social Web, People-Centric*e *Web, Participative Web*.

A Web 2.0 acaba por facilitar propriedades importantes como práticas participativas, colaborativas e distributivas, permitindo que atividades diárias do ser

[44] Cientista Britânico do CERN
[45] Apenas Leitura.

humano, quer numa ótica formal como informal, se transfiram do espaço físico para a Web. Partindo desta premissa, e tendo em consideração as faculdades de escrita e leitura de dados que a segunda geração da Web permite, torna a sua versão 2.0 bidirecional, na medida em que estimula a participação do utilizador na criação de conteúdos e informação, passando de um sujeito passivo (apenas consultava), a ativo (consulta e produz). Desta forma, a segunda geração da Web configura novos modelos de interconexão e interação entre diferentes sociedades, pessoas e as tecnologias e sistemas da informação, permitindo uma relação entre a experiência humana e a tecnologia (Choudhury, 2014).

Na mesma corrente de evolução e desenvolvimento da Web 2.0 surge a terceira geração, ou Web 3.0. Também denominada de Web Semântica tem como objetivo principal impulsionar a evolução da Web atual, facilitando a procura e partilha. A Web semântica, como originalmente concebida, é um sistema que visa dotar a tecnologia a responder aos pedidos humanos complexos com base no seu significado (Choudhury, 2014).

A ideia estruturante da Web 3.0 é definir o conceito "estrutura de dados", permitindo a sua interconexão por forma a otimizar a descoberta, automação, integração e reutilização ao longo das variadas aplicações. Visa vincular, integrar e analisar dados de um conjunto de informação para obter um novo fluxo de informações. É capaz de melhorar a acessibilidade da internet móvel e, por consequência, o fenómeno da globalização, potencializando e enfatizando a satisfação dos seus clientes, bem como na ajuda a estruturar e a colaboração na *Social Web* (Web 2.0) (Aghaei, Nematbakhsh, & Farsan , 2012).

Segundo Dias (2014), a Web 3.0 utiliza Inteligência Artificial (IA), uma vez que tem a capacidade de armazenar e interpretar informação sobre os seus utilizadores, bem como as interações entre estes. Esta capacidade, aliada à IA, incorporada no seu *software,* permite o cruzamento de dados entre si, e consequentemente, a descoberta de padrões e definir perfis de utilizadores, o que possibilita um ajustamento do seu desempenho em função dos mesmos.

A evolução da tecnologia Web, nomeadamente da primeira para a segunda geração veio alterar por completo a maneira como as pessoas comunicam e se relacionam na internet. Associado a esta alteração, está um crescimento exponencial da utilização de plataformas e aplicações, cuja finalidade é a sociabilidade, denominados de *social media.* A utilização das referidas aplicações requer um processo de correlação entre o utilizador e os instrumentos ao seu dispor para a criação de conteúdos. Desta forma, qualquer

utilizador pode inclusivamente utilizar conteúdos criados por outros utilizadores, através de um comentário, acrescento ou partilha (Postman, 2008).

Outros autores como Kaplan & Haenlein (2010) mencionam que a Web 2.0 é a estrutura tecnológica que promove e suporta os *social media*, que são um conjunto de aplicações e plataformas com base na internet, que encaixam na estrutura tecnológica e ideológica da Web 2.0.

Os *social media* podem ser divididos em seis grupos, sendo eles: " Blogs; Sites de Redes sociais (*Facebook);* Projetos colaborativos (*Wikipédia)*; Comunidades de conteúdo (*Youtube)*; Mundos de jogos virtuais (*World of Warcraft)*; Mundos sociais virtuais (*Second Life*)" (Kaplan & Haenlein, 2010, p. 62).

Dado o objeto de investigação é assim que chegamos às redes sociais, que se definem como "aplicações cuja principal finalidade é promover a comunicação, a sociabilidade e o *networking*[46], através da facilitação da criação, da manutenção e da eventual intensificação das relações interpessoais e sociais" (Dias, 2014, p.30). De acordo com Coutinho (2014), a definição de rede social está intima com o conceito de utilizador, pois uma plataforma só poderá ser considerada uma rede social se tiver a figura do perfil, tendo o seu centro de gravidade nas relações que se formam entre estes.

As redes sociais podem categorizar-se em quatro funcionalidades diferentes, que são: "(1) funções relacionadas ao perfil pessoal, (2) funções de relacionamento, (3) funções que permitem aos participantes interagir através de mensagens e comentários, (4) funções para compartilhar informação e conteúdos e (5) funções de identidade que permitem a publicação de informação pessoal, como emoções e estados de ânimo" (Ji et al., 2010, p.81).

Perante tais funcionalidades, percebe-se a influência das redes sociais na vida quotidiana das pessoas, dada a importância na sua vida social. Deste modo, tem-se verificado um adensamento das redes sociais a nível mundial, tendo chegado a 3.196 biliões de utilizadores, representando uma taxa de penetração na população mundial de 42%, de um total de 4.096 Biliões de utilizadores da internet em 2018[47], o que representa uma taxa de 53% referente á mesma população.

No caso específico de Portugal[48], os números representam uma maior taxa de penetração na população, quer na utilização da internet (7,2 Milhões, a uma taxa de 70%),

[46] Estabelecer ligações e relações através da criação de redes.
[47] Ver figura 1.
[48] Ver figura 2.

quer das redes sociais (6,1 Milhões, a uma taxa de 59%). Estes números adquirem um significado maior se tivermos em conta que, 5,2 milhões de utilizadores utilizam as redes sociais através de dispositivos móveis (taxa de penetração de 51%), navegando em média seis horas e dezassete minutos (06H55min) por dia, no computador ou *tablet,* acrescido de uma hora e cinquenta minutos (01H55min) no *smartphone*, sendo que do somatório destas duas parcelas, resulta uma utilização diária das redes sociais de duas horas e dezoito minutos (02H18min).[49]

Dadas as taxas de utilização das redes sociais, é percetível a importância das redes sociais na sociedade e nos seus atores, pois:

> "sites como o Facebook não são apenas um novo terreno onde a vida social ocorre, mas também uma ferramenta para pesquisar e localizar a vida social. Por outras palavras, as interações, relações, eventos e outras características da vida social são mediadas nas redes sociais, tornando-as um tipo de informação mais visível e utilizável" (Trottier, 2012, p. 23).

No entanto, a informação por si só, necessita de uma pesquisa e tratamento para efetivamente se tornar viável e passível de ser utilizada. É então que surge a necessidade de um modelo de monitorização policial nas redes sociais, pois é amplamente reconhecido que os fluxos de dados resultantes da atividade nas referidas plataformas são públicos e, portanto, podem fornecer informações valiosas e acionáveis para apoiar a compreensão situacional e a tomada de decisões. (Preece et al., 2018).

1.4. Monitorização Policial das Redes Sociais

As polícias utilizam as redes sociais essencialmente com dois propósitos: (1) disseminar informação e comunicar com a sociedade; (2) recolher informação destas plataformas tendo por objetivo a prevenção e investigação criminal. Nesta última medida existe um elemento essencial, que são as informações. Para que a informação adquira valor "policial" é necessário a sua análise e tratamento (Community Oriented Policing Services & Police Executive Research Forum [COPS;PERF], 2013).

A monitorização e pesquisa de informação na internet e nas redes sociais pode ser conduzida segundo duas maneiras distintas. A forma administrativa analisa como são utilizadas, por quem, qual o propósito, qual a audiência visada, através de que conteúdos e quais os efeitos que se visa prosseguir [50]. Por outro lado, a abordagem crítica da utilização

[49] Ver figura 3.

[50] Teoria de comunicação de Lasswell. Descreve um processo de comunicação através da definição de quem disse, o que foi dito, qual o seu propósito, amostra alvo e quais os seus efeitos.

da internet, estende-se para além daquilo que é a versão digital da teoria de comunicação de Lasswell. Esta vertente não exclui estudar empiricamente os pilares da utilização da internet e das redes sociais, mas sempre numa ótica de situar a sua investigação na teorização e análise de contextos macro, tais como as estruturas de poder, o Estado, o capitalismo, as relações de género, lutas sociais e ideológicas, que acabam por moldar e ser moldadas tanto pela internet, como pelas redes sociais (Fuchs, 2008).

A rápida e generalizada utilização das redes sociais, representam a maior mudança de paradigma na forma como as pessoas estão a utilizar e a partilhar a informação. É então no âmbito da prevenção de fenómenos criminais que surge o interesse das FSS nas redes sociais, pois é amplamente reconhecido que os fluxos de informação das redes sociais podem fornecer informações valiosas e informações acionáveis para apoiar a compreensão situacional e a tomada de decisões (Lyon, 2001).

Embora seja geralmente reconhecido que confiar nas *social media,* para proporcionar uma compreensão geral e equilibrada de uma determinada situação, é altamente arriscado, quer ao nível demográfico[51], quer em termos da qualidade e validade da informação recolhida, o seu valor como fonte de *insight*[52] pode e deve ser relacionado com outras fontes para atingir a compreensão situacional (Preece et al., 2018).

Monitorização policial é o termo que define o processo de deteção e prevenção do crime, através do Estado e de cada individuo [53] (Newburn, 2011). No caso da monitorização das redes sociais, cada um dos atores enunciados tem o seu papel a desempenhar, com igual grau de importância, sendo indissociáveis e interdependentes para uma monitorização efetiva e eficiente (Williams et al., 2013).

Relatórios de análise à ocorrência de distúrbios civis de grande magnitude, posteriores à introdução do *smartphone*, revelam que a facilidade de circulação e partilha de informação e interação grupal proporcionada pelas redes sociais, são uma das principais causas da elevada complexidade verificada nos tumultos. Uma análise próxima da cronologia de eventos revela que as redes sociais não são utilizadas simplesmente para coordenar, mas também para recrutar, inflamar e incitar o comportamento violento e tumultuoso (Williams et al., 2013).

[51] A amostra pode não ser representativa.
[52] Discernimento e conhecimento da situação
[53] Denuncia de atividades criminosas, partilha de informação em tempo real.

1.4.1 Indicadores de Tensão Social

Em 1981 os distúrbios civis em várias cidades do Reino Unido, com particular incidência para Londres, trouxeram pela primeira vez à ribalta, a capacidade das FSS em antecipar distúrbios de ordem pública. No entanto, só em 2000 é que a *Association of Chief Police Officers*[54] (ACPO), através do *Manual of Guidance on Keeping the Peace* (2000), faz a recomendação para a monitorização de sinais de tensão como forma de antecipar e prevenir incidentes de ordem pública (Association of Chief Police Officers [ACPO], 2000).

Estes indicadores de tensão podem incluir sinais sociais, económicos, políticos, religiosos e ambientais. A referida monitorização visa a identificação das causas de tensão na sociedade (e/ou população alvo). Uma vez identificadas, a atuação policial tem por objetivo reduzir essas mesmas causas, prevenindo um escalar da violência e potenciais distúrbios civis. No entanto, a falta de sensibilização dos operadores para a escolha dos indicadores, consoante a localização, o período e a sociedade alvo, bem como a incapacidade técnica das ferramentas utilizadas, revelaram a incompetência de interpretação dos indicadores por parte das FSS para uma intervenção preventiva (ACPO, 2000).

Inicialmente, os indicadores de tensão foram assumidos como sendo visíveis e, portanto, facilmente monitorados. Para a grande maioria das FSS, a observância dos mesmos resultava daquilo que eram as estatísticas criminais convencionais[55] (Chainey, 2008).

As dificuldades sentidas nesta matéria foram enfatizadas pelos distúrbios na cidade de Burnley. Os distúrbios civis nesta cidade inglesa resultaram da falta de capacidade da Força de Segurança (FS) , territorialmente competente para a leitura de indicadores de tensão, especificamente, o significado pleno do sentimento racista e xenófobo da população nativa, perante a crescente comunidade asiática que se estabelecia na cidade. O aumento da consternação social e medo no seio dessa comunidade, em virtude da pressão racista imposta, conduziu a uma reação que esteve na base dos distúrbios civis (King & Waddington, 2004).

---

[54] É uma associação não governamental, constituída por oficiais de Polícia, com o objetivo de desenvolver práticas policiais adequadas.

[55] Estatísticas de Criminalidade constantes em relatório de natureza idêntica ao Relatório anual de Segurança Interna (RASI).

Os vários relatórios policiais dos distúrbios civis ao longo do ano de 2011 em várias cidades inglesas e canadianas enfatizaram a necessidade de se estabelecer um centro de informações com capacidade preditiva em relação a focos de distúrbio da ordem pública. A produção de informações policiais, seria resultado do tratamento e correlação de dois fluxos de informação distintos, o das redes sociais e dos agentes em atividade operacional (Burnap, Williams, Morgan, & Housley, 2014). No que se refere às redes sociais, o sistema de monitorização, através da recolha massiva de dados nestas plataformas, permitiria analisar as tendências de tensão social em função de um determinado tópico/tema ou comunidade. A conexão entre a informação proveniente das redes sociais e dos agentes em atividade operacional, contribuiria decisivamente para uma melhor compreensão do ambiente operacional (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services [HMIC], 2011).

Na sua génese este centro de informações deparou-se com vários problemas na recolha e tratamento dos dados recolhidos através da monitorização das redes sociais. O fluxo de dados recolhido era de uma ordem de grandeza tal, que tornava impraticável qualquer tipo de processamento e análise. Existia também uma grande dificuldade em separar o trigo do joio, ou seja, analisar e perceber quais os dados que poderiam ser tratados e convertidos em informações policiais, bem como aqueles em que o seu conteúdo continha informação errada e/ou enganosa (Williams et al., 2013).

A informação recolhida através do sistema de monitorização das redes sociais são de difícil interpretação, particularmente pelo empobrecimento dos dados recolhidos no que concerne aos *metadata*[56]. A carência destes elementos, aliado à dificuldade de interpretar dados que raramente progridem de um rumor para um "status" de informações policiais, com a capacidade preditiva, falhou na incumbência de antecipar acontecimentos potencialmente disruptivos da ordem e tranquilidade pública (Schneider & Trottier, 2012).

Perante esta incapacidade, surgiu a necessidade de reunir um conjunto de especialistas, nas áreas da sociologia, criminologia e informática. A tarefa desta equipa era contruir um sistema de monitorização de tensão social nas redes sociais, com base em conceitos sociológicos que permitissem o seu desenho em linguagem informática para operar um ambiente digital. Este algoritmo foi então capaz de identificar sinais de tensão social em determinadas comunidades, o que permitiu a sua quantificação sob forma de indicadores (Williams et al., 2013).

[56] Os *meta-dados* são dados relacionados com a identidade dos utilizadores, nomeadamente, hora da publicação, IP e localização.

1.4.2 Taxionomia sentimental

A análise de informação proveniente das redes sociais tem o seu expoente máximo quando se fala em taxionomia de sentimentos. Esta conjugação resulta da associação entre as palavras e o seu significado em termos sentimentais. A plataforma *Sentinel*[57] é pioneira neste âmbito e foi desenhada segundo uma abordagem baseada num conhecimento pré-estabelecido, no qual, os fluxos de entrada, são caracterizados por parâmetros geográficos, culturais, etnológicos e sociais previamente conhecidos. Associado a estas características, está uma terminologia própria que varia em função das mesmas. Através da criação de um algoritmo informático próprio, toda a informação que é recolhida, é marcada e inserida num sistema de taxionomia, em que cada palavra e/ou conjunto de palavras tem associado um determinado comportamento e/ou sentimento. Estas associação é feita segundo teoremas de ontologia (Preece et al., 2018).

Sempre que existe uma associação a um sentimento conotado negativamente é emitido um alerta. Cada caso destes é analisado de forma individualizada por um analista, com base numa *framework* de quem, o que, quando, onde e porque? (Preece et al., 2018).

A aplicação deste modelo adequa-se melhor a situações já conhecidas, como eventos ou comunidades minoritárias, uma vez que os seus resultados ajudam em muito à compreensão situacional e perceção da realidade social num determinado contexto. Esta plataforma é um exemplo perfeito da correlação entre informáticos e sociólogos no que concerne à monitorização das redes sociais (Williams et al., 2013).

1.4.3 Discurso de Ódio

O discurso de ódio é um conceito emocional, para o qual não existe uma definição universalmente aceite, naquilo que é o Direito Internacional. Apesar de ser facilmente identificável, o critério utilizado é normalmente indiscritível ou contraditório (Article 19 [A19], 2015).

No entanto, é possível definir a palavra "ódio" como "sentimentos e crenças extremamente negativas sobre um determinado grupo ou um representante deste em virtude da sua raça, etnia, religião, género ou orientação sexual" (Ring, 2013, p. 14). Associando esta definição à pratica, podemos entender o discurso de ódio como uma forma de "promover, incitar, promover ou justificar ódio racial, xenofobia, antissemitismo ou

[57] Ver Anexo B– Figura 4

outras formas de ódio baseado na intolerância, discriminação e hostilidade contra minorias" (Ring, 2013, p. 14).

As redes sociais constituem-se como uma plataforma ideal para a prática do discurso de ódio dado o grau de anonimização que confere aos seus utilizadores. Este flagelo já despertou o interesse de organismos responsáveis pela proteção dos Direitos Humanos e dos próprios SMS, por forma a inibir e restringir esta prática (A19, 2015).

A pirâmide do discurso de ódio[58] faz uma relação entre o tipo de discurso, a sua gravidade, as medidas a tomar e os instrumentos de Direito Internacional infringidas.

Quando o discurso de ódio utilizado se refere a termos relativos a intolerância[59], tem de ser controlado e as suas vitimas protegidos. Situações em que a segurança, ordem pública e/ou saúde publica[60] são postas em causa pelo discurso de ódio, devem ser tomadas ações com o objetivo de restringir a sua prática e apagado o seu conteúdo. Sempre que seja feita menção a atos de violência ou discriminação em virtude de discriminação[61], os comentários têm obrigatoriamente que ser restringidos (A19, 2015).

1.5 Informações Policiais

Segundo Pereira (2013) na sociedade hodierna, o conhecimento constitui um fator estratégico na gestão operacional das FS, cabendo às informações nortear a ação policial, promovendo a predição da ilicitude e o cumprimento da legalidade e ordem pública (Clemente, 2008).

Antes de entrar no campo das informações é preciso entender o conceito de dado e informação. Os dados são observações documentadas ou resultados de uma medição sem qualquer valor contextual. Já o conceito de informação difere do contexto de análise em que está inserido. Na presente investigação considera-se informação como um "conjunto de dados que foram categorizados ou colocados segundo padrões de classificação (...) que quando fornecido de forma atempada, melhora o conhecimento da pessoa que o recebe, ficando ela mais habilitada a desenvolver determinada atividade ou tomar determinada decisão" (Vaz, 2015, p. 43) (Amaral, 1994, p. 25).

Desta forma, salienta-se que os dados são "simples observações, livres de sentido adicional, inferência ou opinião" (Ratcliffe, 2008, p. 96), e que a informação é o conjunto

[58] Ver anexo C – Figura 5.
[59] Infringe o art.º 19º da Convenção Internacional de Direitos Civis e Políticos (CIDCP).
[60] Infringe o nº3 do art.º 19º da CIDCP.
[61] Infringe o nº2 do art.º 20º da CIDCP.

de dados a que o observador considerou suficientemente importantes e relevantes para o seu processo de tomada de decisão (Vaz, 2015).

Estando num patamar superior, as informações resultam do tratamento e análise da informação, por forma a atribuir-lhe um significado no quadro de atuação a que se destina. É um processo de congregação e compreensão contextualizada da informação relacionada e organizada (United States [US] Army , 2010). Ou seja, "as informações podem ser definidas como um produto de valor acrescentado, derivado da recolha e análise de toda a informação relevante (...) que é imediata ou potencialmente significativa para a tomada de decisão (...)" (Peterson, 2005, p. 6).

No âmbito da presente investigação torna-se necessário fazer uma distinção entre os dois tipos de informações com particular relevância para as FS: as informações de segurança e informações policiais.

Moleirinho (2009, p.81) refere que:

> "as informações de segurança têm como destinatários os órgãos de decisão política ou as chefias de topo das autoridades policiais, revestindo um carácter transversal que engloba fatores macroeconómicos, sociais, políticos e culturais, que abrangem dimensão regional, nacional e mesmo internacional, podendo assumir uma natureza meramente estratégica ou também operativa."

Dadas as suas características, as informações de segurança inserem-se no quadro de atuação do Sistema de Informações da República Portuguesa (SIRP) (Assembleia da Républica [AR], 2014).

Numa ótica voltada para uma vertente operacional surge o conceito de informações policias, que se revestem de particular importância para esta investigação, uma vez que são "aquelas destinadas à prossecução das missões policiais legalmente suportadas, num nível instrumental, mais estratégico-operativo, com o fim de suportar a atividade das estruturas operacionais" (Torres, 2005, p. 593).

Segundo Clemente (2008) as informações policiais dividem-se em três sub-categorias, as de ordem pública, criminais e contrainformações.

"As primeiras têm na génese da sua produção a prevenção criminal e de incidentes de ordem pública; as segundas, por seu turno, inserem-se no âmbito de um (...) processo-crime; e as últimas visam garantir a segurança nacional e produzir informação ao nível estratégico, obstando, entre o mais, também ações hostis de recolha de informação sobre as capacidades, objetos e vulnerabilidade nacionais" (Moleirinho, 2009, p. 81).

Perante esta categorização, torna-se bastante esclarecedor que monitorização policial das redes sociais está diretamente relacionada com a produção de informações de

ordem pública, uma vez que estas "visam a prevenção de incidentes de ordem pública e acautelar a ocorrência de incivilidades, em particular a produção de delitos criminais (...)" (Clemente, 2008, p. 24).

As informações policiais, quando produzidas com propriedade, podem constituir-se como uma ferramenta auxiliar e preponderante na prevenção criminal, sendo esta uma "função primordial e prioritária em qualquer Estado de direito democrático, cabendo em especial às FS envidar os necessários esforços para evitar a ocorrência de factos atentatórios das finalidades da atividade de segurança interna através da dissuasão, vigilância e controlo (...)" (Torres, 2005, p. 585).

1.5.1 Policiamento Orientado pelas Informações

Segundo Ratcliffe (2008, p. 6) "quando foi proposto pela primeira vez, o Policiamento Orientado pelas Informações (POI) era uma tática operacional que iria reduzir o crime através de um policiamento proactivo apontado por informações criminais."

O aumento da criminalidade, em frequência e complexidade, foi o grande catalisador para adoção deste modelo de policiamento. O decréscimo dos meios disponíveis veio também contribui para adoção do POI, mudando o foco da criminalidade geral para a especifica. Fruto desta mudança, foram identificadas quatro prioridades táticas para o POI: (1) *targeting* de atividade criminais; (2) gestão de locais de risco; (3) aplicação de medidas preventivas tendo em vista a redução da criminalidade e desordem pública (Jerry, 2003).

De acordo com Fuentes (2006, p. 3):

> "o policiamento orientado pelas informações é uma filosofia colaborativa que começa com informação, recolhida em todos os níveis da organização que é analisada para criar informações úteis e uma percepção melhorada do ambiente operacional. Isto vai assistir a liderança a efetuar as melhores escolhas possiveis em relação à prevenção criminal, alocação de recurso e operações táticas."

Numa sociedade cada vez mais dependente da internet e das redes sociais, a vigilância social exercida através da monitorização policial das referidas plataformas pode tornar-se numa ferramenta essencial para este tipo de policiamento, uma vez que este modelo requer analistas devidamente formados para proceder à interpretação do ambiente operacional e que usem as informações policiais para direcionar tática e operacionalmente as medidas de policia, pois "o POI trata-se de uma técnica concetual com uma dimensão eminentemente instrumental, não se configurando como o produto final do policiamento,

mas como um meio para ser atingida uma melhor eficiência e eficácia na ação policial" (Elias, 2009, p. 758).

CAPÍTULO 2
ENQUADRAMENTO METODOLÓGICO

2.1 Metodologia e Procedimento

No âmbito das ciências sociais, a utilização do método científico[62] é essencial, por forma a prosseguir "os objetivos de medição, tendo em vista reproduzir e aplicar conhecimentos julgados úteis e mesmo predizer os seus efeitos" (Freixo, 2012, p. 171).

A metodologia adotada é fundamental para a resolução da problemática, pelo que o método cientifico, enquanto "conjunto de procedimentos intelectuais e técnicas adotadas para se atingir o conhecimento" (Gil, 2008, p. 8), constitui um elemento estruturante e de suporte ao processo[63] de investigação. Este "conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo – conhecimentos válidos e verdadeiros – traçando o caminho a ser seguido, detetando erros e auxiliando as decisões do cientista" (Marconi & Lakatos, 2003, p. 83).

2.1.1 Método de Abordagem

De acordo com Sarmento (2013), o método de abordagem à problemática em causa consiste no dedutivo, através do qual "a razão é capaz de levar ao conhecimento verdadeiro, que decorre de princípios *a priori* evidentes e irrecusáveis" (Gil, 2008, p. 9).

De facto, este método de abordagem é aquele que mais se adequa a esta investigação, uma vez que se procura uma "compreensão absoluta e ampla do fenómeno em estudo" (Fortin, 2009).

O raciocínio dedutivo intenta explicar o conteúdo das premissas, através de uma cadeia de raciocínio numa estrutura descendente, analisando do geral para o particular, com o intuito de construir uma conclusão (Fortin, 2009).

Desta forma, optamos por uma abordagem qualitativa à problemática, tendo por base duas premissas essenciais. A primeira envolve a migração da vida social do espaço físico para o ciberespaço, essencialmente através das redes sociais, sendo que a segunda tem que ver com as potencialidades da monitorização das redes sociais num âmbito

[62] Ver apêndice D – Desenho de estudo.
[63] Ver apêndice B – Quadro Relação

policial, sobre as quais foi recolhida informação com "o propósito de explicar o conteúdo das premissas" (Marconi & Lakatos, 2003, p. 92).

2.1.2 Base Lógica da Investigação

Pretendemos com esta investigação alertar para a necessidade da monitorização das redes sociais, em função do contexto social[64] em que nos encontramos. Para tal, é necessário caracterizar esta atividade naquilo que é a matriz policial, identificar o espetro de atuação da GNR neste âmbito, perceber quais as debilidades a mitigar e as capacidades a desenvolver.

A análise do modelo de monitorização das redes sociais por parte da GC deve-se ao facto de a realidade cultural, social e económica espanhola ser bastante similar à portuguesa. No entanto, o contexto politico e histórico é bastante diferente, o que coloca desafios de ordem e tranquilidade pública, paz social, proteção das instituições democráticas e do próprio Estado à GC, que não se colocam à GNR, ou pelo menos com uma dimensão igualitária.

Apesar de estas duas forças de segurança serem congéneres e partilharem a mesma condição militar, a sua organização e orgânica são distintas, em parte, devido às atribuições e missões que estão adstritas a cada uma delas.

Este paradoxo entre semelhanças e diferenças explanadas nos parágrafos suprarreferidos, faz do modelo de monitorização das redes sociais desenvolvido pela GC um exemplo de análise e compreensão para a GNR. Por um lado, a realidade sociocultural é bastante semelhante, por outro, lida com situações de uma maior magnitude e complexidade do que aquelas que normalmente se regista em Portugal. Este facto, juntamente com a diferença de competência na investigação criminal, enfatiza a adequação da análise do modelo de monitorização das redes sociais da GC, ao mesmo tempo que afasta uma análise comparativa.

2.1.3 Objetivos e Modelo de Análise

A formulação de questões de investigação concorre diretamente para a prossecução dos objetivos definidos e consequente elucidação do problema de investigação, que deve "definir o fenómeno em estudo através de uma progressão lógica de elementos, de relações, de argumentos e de factos" (Fortin, 2009, p. 62).

[64] Utilização massiva das redes sociais.

Tendo por finalidade "combinar o problema e o objetivo numa explicação ou predição clara dos resultados esperados" (Fortin, 2009, p. 102), foi formulada, enquanto elemento estruturante do processo de investigação e "através do qual o investigador tenta exprimir o mais exatamente possível o que procura saber, elucidar e compreender (...) (Quivy & Campenhoudt, 2013, p. 48), a seguinte questão central:

QC: Que modelo de monitorização policial das redes sociais deve ser desenvolvido pela GNR?

Por forma a dar resposta à problemática colocada, foram definidos objetivos específicos, materializados nas seguintes questões derivadas:

QD1: Quais as características essenciais da monitorização policial nas redes Sociais?

QD2: Em que espectro de atuação se insere a monitorização policial das redes sociais pela GNR?

QD3: Que capacidades deve a GNR desenvolver e potenciar, no âmbito da monitorização policial das redes sociais?

QD4: Como se caracteriza o modelo de monitorização policial das redes sociais desenvolvido pela *Guardia Civil*?

2.1.4 Caracterização e Justificação da Amostragem

A amostra é a "porção ou parcela, convenientemente selecionada do universo (população)" (Marconi & Lakatos, 2003, p. 223) . A escolha da mesma foi baseada num método não probabilístico, denominado amostragem por seleção racional, pois "baseia-se na seleção pelo investigador de determinados sujeitos em função de características típicas" (Freixo, 2012, p. 212), sendo selecionadas "as unidades de amostragem a partir de critérios específicos" (Aires, 2011, p. 22).

Perante o âmbito da investigação foram constituídos quatro grupos de entrevistados[65].

No Grupo 1 temos académicos que dedicaram o seu percurso profissional à análise de fenómenos sociais e à ação das FSS com base nas redes sociais, tendo uma vasta experiência no contexto da monitorização das referidas plataformas num contexto policial.

O grupo 2 é dedicado a especialistas que ocupam cargos de direção e chefia na área do cibercrime, nomeadamente na Policia Judiciária e no gabinete do cibercrime da

[65] Ver Apêndice C – Lista de Entrevistados

Procuradoria-Geral da República, essenciais para perceber a problemática do cibercrime e criminalidade tecnológica cometida através das redes sociais.

No grupo 3 temos um conjunto de especialistas que desempenham funções na GNR ou em organismos externos em comissão de serviço, nomeadamente nas áreas das informações, investigação criminal, comunicação e cibersegurança.

A amostra do grupo 4 é constituída em exclusivo por elementos da GC, com experiência profissional ao nível da *Jefatura de Informácion*[66] *e Jefatura de Policia Judicial*[67], bem como conhecimentos na monitorização das redes sociais no âmbito da prevenção e investigação criminal. Derivado da sua situação politica, o Reino de Espanha, tem a sua história marcada por movimentos separatistas e independentistas, que em algumas situações acabavam por ter um braço armado amplamente conotado com ações terroristas. Esta situação de ameaça terrorista adensou-se aquando dos atentados terroristas na cidade de Madrid[68]. Perante esta ameaça, a GC desenvolveu várias estruturas de investigação, combate e prevenção do terrorismo. Neste âmbito, as redes sociais constituem-se como um dos meios primordiais para o ciberterrorismo, e, por conseguinte, uma área de atuação essencial na recolha de informações. O *know how* adquirido nesta matéria e a sua potencialidade levou a GC a ampliar a monitorização das redes sociais a todas as suas áreas de atuação, constituindo-se como um modelo de referência.

2.2 Técnica de Recolha de Dados

Os instrumentos de investigação determinam a forma de recolha de dados por parte do investigador, pois "a natureza do problema de investigação determina o tipo de método de colheita de dados a utilizar. A escolha do método faz-se em função das variáveis e da sua operacionalização(...)" (Fortin, 2009, p. 239). Assim, entende-se a recolha de dados como "um processo organizado, posto em prática para obter informações junto de múltiplas fontes com o fim de passar de um nível de conhecimento, para outro (...) ou de representação de uma dada situação" (Freixo, 2012, p. 220).

Numa primeira fase, tendo em vista a elaboração do Capítulo I, foi efetuada uma análise documental das fontes bibliográficas, de forma explanar aquele que é o estado da arte da temática em questão, desenvolvendo um quadro concetual essencial ao

[66] Unidade de policia judiciária responsável pela investigação de crimes contra o Estado

[67] Unidade de policia judiciária responsável pela investigação do restante catálogo de crimes.

[68] Ataque terrorista reivindicado pela Al-Qaeda na estação ferroviária de Atocha em 11 de março de 2004, tendo sido registados 141 mortes e mais de 1800 feridos.

desenvolvimento da investigação. Perante a natureza da mesma, os documentos consultados são essencialmente de suporte digital, mas também em suporte físico, nomeadamente, livros e publicações académicas.

A segunda fase baseia-se na "recolha de dados a partir de experiências, (...) entrevistas (...), que o investigador ou outras pessoas experienciaram ou tem conhecimento relevantes e fidedignos sobre o tema em análise" (Sarmento, 2013, p. 10).

A entrevista foi o método escolhido para a recolha de dados na segunda fase da investigação, uma vez que possibilita complementar a análise documental através da "obtenção de dados que não se encontram em fontes documentais e que sejam relevantes e significativos" (Marconi & Lakatos, 2003, p. 198), permitindo "explorar um domínio e aprofundar o conhecimento através da inquirição presencial a um ou mais indivíduos" (Sarmento, 2013, p. 28).

As entrevistas realizadas são do tipo semidirectivo, ou semidirigida, "no sentido em que não é inteiramente aberta" (Quivy & Campenhoudt, 2013, p. 193).

Dentro deste tipo, surge a entrevista de especialistas, em que a "interpretação da entrevista de especialidade tem como principal objetivo analisar e comparar o conteúdo dos conhecimentos do perito" (Flick, 2005, p. 93). Perante esta tipologia de entrevistas pretende-se que a informação recolhida tenha por base, o conhecimento e a experiência profissional adquirida na área especifica, na qual o entrevistado desenvolve a sua atividade.

É perante este pressuposto de especificidade que foi elaborado o quadro de entrevistados[69], tanto ao nível dos diversos grupos de entrevistados constituídos, como nas áreas de especialização dentro do grupo 3 e 4.

As entrevistas foram elaboradas e apresentadas através de um guião[70] com base no quadro modelo[71] de entrevista.

2.3Tratamento e Análise de Dados

Segundo Quivy & Campenhoudt (2008, p.185), "os métodos de recolha e os métodos de análise são normalmente complementares", o que no caso da entrevista, "requer habitualmente métodos de análise de conteúdo" (Quivy & Campenhoudt, 2013, p. 185). Este tipo de análise qualitativa "procura adequadamente as respostas às perguntas

[69] Ver apêndice C – Lista de Entrevistados.
[70] Ver apêndice A – Carta de apresentação e guião da entrevista.
[71] Ver apêndice B – Quadro Relação.

com base na análise de vários contextos sociais e dos indivíduos que a eles pertencem" (Berg, 2001, p. 6), tendo como objetivo "descrever ou interpretar, mais do que avaliar" (Freixo, 2012, p. 173).

Para o efeito, e tendo por base o modelo de análise de conteúdo desenvolvido por Guerra (2006), foram elaboradas sinopses das entrevistas em quadros de análise para cada uma das questões[72].

"As sinopses são sínteses dos discursos que contêm a mensagem essencial da entrevista e são fiéis, inclusive na linguagem, ao que disseram os entrevistados. Trata-se, portanto, de material descritivo que, atentamente lido e sintetizado, identifica as temáticas e as problemáticas" (Guerra, 2006, p. 73).

"Têm como objetivos centrais: Reduzir o montante de material a trabalhar, identificando o *corpus* central da entrevista; permitir o conhecimento da totalidade do discurso, mas também das suas diversas componentes; facilitar a comparação longitudinal das entrevistas; ter a perceção da saturação das entrevistas" (Guerra, 2006, p. 73).

[72] Ver apêndice E – Análise Qualitativa dos Resultados.

CAPÍTULO 3
APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

Pretendemos, neste capítulo, apresentar e sintetizar os aspetos fundamentais das respostas dos entrevistados através das sinopses.[73] Tendo em vista a simplicidade e objetividade da análise e discussão dos resultados, as quinze perguntas que compõem o guião da entrevista[74] são apresentadas individualmente em quadros[75] de análise qualitativa, congregando as respostas de toda a amostra.

Desta forma, a análise e discussão de resultados é feita através da comparação entre a informação explanada no enquadramento teórico e o conhecimento obtido através do tratamento das entrevistas.

3.1 Apresentação, análise e discussão da questão nº1

Através desta questão pretendemos identificar e caracterizar o quadro de atuação das FSS na monitorização das redes sociais.

Existe a clara perceção que a monitorização das redes sociais, enquanto principal fonte de OSINT (E2; E8), deve estar essencialmente baseada na recolha de informação que, após tratada e analisada, pode constituir-se como uma ferramenta de prevenção criminal e preditiva na perceção da realidade social num âmbito de ordem e tranquilidade pública (E1, E2, E4, E5, E6, E7, E8).

No estudo dos distúrbios civis na cidade de Vancouver esta realidade ficou bastante patente. Trottier (2012) ressalvou a necessidade de conjugar e correlacionar, as informações produzidas a partir das redes sociais com a informação recolhida pelos operacionais no terreno, uma vez que só assim se tornaria possível ter uma perceção do ambiente operacional.

No entanto, ao nível da prevenção criminal não existe uma forma regular ou organizada de monitorização das redes sociais (E3).

---

[73] Seleção de excertos mais importantes.
[74] Ver apêndice A – Carta de Apresentação e Guião da Entrevista
[75] Ver apêndice E – Análise Qualitativa das Entrevistas

Esta atividade é também condizente com a investigação criminal e recolha de prova digital[76]. (E3, E4, E6).

O quadro de atuação das FSS nas redes sociais visa a obtenção de informações de segurança e/ou policiais (E8). Segundo Moleirinho (2009) as informações de segurança, dado o seu valor estratégico, são uma atribuição dos serviços de informações. Por outro lado, as informações policiais, nomeadamente as de ordem pública e criminais, são uma parte fundamental do policiamento orientado pelas informações (Clemente, 2008).

Na perspetiva da comunicação institucional são definidas estratégias de transmissão de conteúdos em função dos seguidores e dos temas atuais, por forma a tornar a comunicação cada vez mais eficiente (E9).

3.2 Apresentação, análise e discussão da questão nº2

Nesta questão pretende-se compreender como a monitorização das redes sociais se pode constituir como uma ferramenta de apoio na prevenção e combate à criminalidade.

Hoje em dia muitos dos aspetos da vida social estão associados às redes sociais, dada a sua migração do espaço físico para o ciberespaço (E2; E6). Perante este facto, todos[77] os inquiridos concordam que a monitorização das redes sociais pode ser uma ferramenta essencial na prevenção criminal, uma vez que as FSS têm de se posicionar naquilo que é a nova realidade digital da internet e das redes sociais (E4).

Sendo a prevenção criminal uma função primordial do Estado, a monitorização policial das redes sociais pode tornar-se preponderante na prossecução da mesma (Torres, 2005).

Ao manter uma monitorização permanente e contínua nas redes sociais, vai ser possível perceber quais as suas tendências. Neste contexto, a criação de *ciber-personas*, por forma a monitorizar grupos específicos, é preponderante (E5).

A recolha e análise da informação proveniente das redes sociais, quando associada a outras fontes de informação, e com base num contexto social e local específico, pode tornar-se numa ferramenta muito poderosa para auxiliar na missão de prevenção criminal (E1; E2; E8).

No que concerne ao combate à criminalidade, a monitorização é mais um fator que integra aquilo que será a fórmula de combate à criminalidade, com o objetivo de

[76] Ainda que seja de forma residual.
[77] E1 a E9.

otimização, através de uma economia de meios e utilização de informações para o direcionamento do policiamento. (E7).

A monitorização pode também ser bastante útil naquilo que é a investigação criminal, dado que grande parte dos dados inerentes à prova digital acabam por estar nas redes sociais e nas comunicações subjacentes a todas as interações (E4). No âmbito da Lei do cibercrime e dos pontos de contato para a cooperação internacional, existe uma maior capacidade para fazer a recolha e preservação da prova digital, essencialmente através das medidas processuais previstas no referido diploma legal (AR, 2009).

Muitas das diligências de investigação criminal, que se faziam anteriormente no espaço físico, estão também elas a migrar para as redes sociais, uma vez que atividade criminal de reunião no espaço público é agora efetuada através destas plataformas (E6).

Ao nível da comunicação, as redes sociais constituem como o veículo de excelência para difundir conselhos de segurança (E9).

3.3 Apresentação, análise e discussão da questão nº3

Com esta questão pretendemos perceber como funciona o processo de partilha de informação entre as os ISP, SMS e as autoridades judiciárias em matéria de investigação criminal.

A partilha de informação entre as entidades suprarreferida, sendo preponderante, é uma das principais dificuldades sentidas (E1) para uma monitorização das redes sociais eficiente, com particular incidência para a recolha de prova digital e no decorrer do inquérito criminal (E2, E3, E4, E6). No entanto, existe uma questão legal que se levanta devido aos diferentes ornamentos jurídicos em que estão inseridos (E2 e E7), o que torna o acesso aos *metadata* e ao próprio conteúdo das publicações infrutífero, prática, que também é enfatizada pelos diferentes objetivos e politicas de atuação (E2 e E8) de cada uns dos serviços mencionados em função de cada caso. Este é um dos principais exemplos do fenómeno da privatização da segurança (Militão, 2013).

Apesar dos constrangimentos, os mecanismos de cooperação existem e são cada vez mais eficientes, em virtude da estreita colaboração entre MP e os serviços supramencionadas, devido à criação de canais de contato diretos, aperfeiçoamento de procedimentos (notas práticas) e aumento da força jurídica da legislação europeia. As notas práticas produzidas pelo GCPGR (E3) a sua difusão pelas FSS (E6) e o ponto de contato 24/7 da PJ (E4) são muito importantes nesta problemática.

Nestas notas práticas, são estabelecidos os procedimentos a adotar para num caso de pedido de *metadata* a estes prestadores de serviços.

3.4 Apresentação, análise e discussão da questão nº4

Com esta questão pretendemos perceber o trabalho desenvolvido pela GNR na monitorização das redes sociais.

De uma forma estruturada e bem definida, com base num objetivo claro e de acordo com aquilo que é a missão geral da GNR, a atividade de monitorização das redes sociais por parte desta força de segurança está ainda numa fase muito embrionária. (E5; E6; E8). Ainda assim, existe algum trabalho nesta área, essencialmente ao nível local e de uma forma *ad-hoc* (E5; E6).

Tal como plasmado na estratégia 2020, existe uma visão institucional para aquilo que é a importância desta atividade para a missão geral da GNR, que prevê a criação do CI (E6; E8) estando, neste momento, a ser levantadas as necessidades técnicas e de formação dos recursos humanos (E8), nomeadamente através da aquisição de *software* e de cursos OSINT (E5; E8).

Para além da Estratégia da Guarda 2020, também conceito Estratégico de Segurança Interna identifica como linha de ação estratégica o aumento da capacidade ciber e combate ao cibercrime (Lourenço et al., 2015). No entanto, as medidas operacionais tomadas não estão em consonância com aquilo que é a visão estratégica de segurança interna.

3.5 Apresentação, análise e discussão da questão nº5

Esta questão tem como objetivo compreender de que forma a monitorização das redes sociais contribui para a missão da GNR.

Apesar de se considerar que contribui imensamente para a missão da GNR (E5), uma vez que é cada vez mais visível a migração da vida social do espaço físico (E5; E7) para as redes sociais, o seu contributo ainda é bastante reduzido (E8).

A monitorização constitui-se como uma ferramenta de apoio complementar à missão da GNR, seja através da produção de informações, apoio à investigação através da recolha de prova digital, apoio ao processo de decisão, manutenção da ordem pública e paz social (E6; E7, E8). Todas estas tarefas visam a prevenção e combate à criminalidade, seja ela nas redes sociais ou no espaço físico (E5; E6).

Os maus tratos a animais de companhia são um exemplo claro da importância desta atividade de monitorização, uma vez que grande parte do ativismo é efetuado através destas plataformas (E5).

3.6 Apresentação, análise e discussão da questão nº6

Os objetivos essenciais desta questão estão relacionados com a importância dos indicadores de tensão social para a compreensão da realidade social e como as redes sociais (SOCMINT) podem constituir-se como um medidor de excelência.

A medição de indicadores de tensão social a partir das redes sociais necessita de *software* especializado (E2; E8), de um contexto local e social (E2; E5; E7;) e essencialmente, da sua confirmação ao nível local, através de operativos no ambiente operacional, (E2) bem como, através de outras fontes OSINT (Burnap et al., 2014).

O grande desafio neste contexto, é a escolha dos indicadores a medir de acordo com a realidade que se pretende ter uma perceção do ambiente operacional. Para tal, a monitorização dos indicadores de tensão social tem de obedecer a um conjunto de critérios, como a verossemelhança de quem praticou a publicação, qual o seu contexto, a sua capacidade e a sua intenção (E7). Uma boa escolha deve ser feita de acordo com a localização, período e população e/ou público alvo da monitorização (ACPO, 2000), o que permite desenhar um padrão e perceber quais a tendências (E5).

A principal vantagem da monitorização dos indicadores de tensão, e consequente perceção da realidade social, está diretamente relacionado com situações latentes de ordem pública (E6; E8), nomeadamente cortes de estrada, manifestações e distúrbios civis. Ou seja, uma boa análise dos indicadores de tensão social contribui decisivamente para uma boa compreensão do ambiente operacional (HMIC, 2011).

É, no entanto, necessário ter em atenção que pode haver uma inflamação propositada destes indicadores de tensão social (E1).

3.7 Apresentação, análise e discussão da questão nº7

Em virtude dos normativos legais e o exponencial crescimento do cibercrime e da criminalidade tecnológica, é necessário definir o quadro de atuação da GNR perante esta tipologia de criminalidade.

Quando se reporta a criminalidade tecnológica, a grande maioria dos inquiridos são perentórios a indicar a GNR com clara competência de investigação. No catálogo de

crimes em que a GNR tem a competência de investigação não é a utilização de meios tecnológicos que invalida essa mesma competência (E4; E5; E6; E8). E esta é uma realidade cada vez mais presente, uma vez que a utilização de meios tecnológicos como meio de auxílio na execução dos crimes é cada vez maior e tende a aumentar. (E4; E5; E6; E8).

No entanto, mesmo que exista a utilização do meio tecnológico, cabe perceber se este é um caso isolado, como é o caso da divulgação de conteúdo indevido, ou se é um fenómeno criminal que pode levar a um caso de criminalidade organizada. Caso se verifique este fenómeno criminal, a investigação deve ser da competência da PJ (E4).

Num outro sentido, quando se trata de cibercrime em sentido estrito, existe também uma clara consciência de que a PJ tem a competência reservada da investigação. (E4; E5; E6; E8). Neste âmbito a atuação da GNR prende-se apenas com as medidas cautelares e de policia (E5).

A exponencial utilização de meios tecnológicos e informáticos veio generalizar a necessidade de investigação, o que implica uma adaptação da LOIC neste sentido (E4).

Ao nível da comunicação, a GNR desenvolve um trabalho preventivo neste âmbito, uma vez que divulga nas suas páginas e perfis institucionais conselhos de segurança para situação como *sextortion*[78] e burlas online. Por outro lado, sempre que existe uma denúncia através das redes sociais a mesma é reencaminhada via canal hierárquico ao Comando Operacional (CO) (E9).

3.8 Apresentação, análise e discussão da questão nº8

Com esta questão, pretendemos identificar quais as capacidades que devem ser edificadas e desenvolvidos no âmbito da monitorização policial das redes sociais por parte da GNR.

Inicialmente é necessário desenvolver uma *Framework*, ou seja, um quadro organizacional. Para tal, é necessário definir estrategicamente os objetivos da monitorização e perceber qual contribuição cada missão específica da GNR. Perante estes pressupostos, é também necessário definir qual a sua dependência orgânica e funcional (E7).

Mais do que questões técnicas e equipamento, é necessária uma componente fortíssima de sensibilização e formação dos recursos humanos (E5; E6; E7; E8).

[78] Divulgação de conteúdo sexual na internet como forma de vingança ou de chantagem/extorsão.

É essencial uma sensibilização de todos os militares para as potencialidades da utilização destas plataformas, seja ao nível da prevenção ou investigação criminal, sendo os cursos base o veiculo primordial para tal (E5; E6).

Ao nível da formação é preciso dotar o quadro de recursos humanos que vão trabalhar nesta área de especialistas, na área da sociologia, teoria comportamental, informática e estatística. (E5; E7).

A contratação de especialistas nas áreas suprarreferidos, foi um dos fatores decisivos no sucesso de desenvolvimento de ferramentas técnicas de recolha e análise de informação (Williams et al., 2013). A correlação das ciências sociais com a informática é um fator crítico de sucesso (Preece et al. 2018).

No que concerne à investigação criminal é necessário sensibilizar os militares para a importância da prova digital (E6).

Para perceber que capacidades desenvolver no âmbito da monitorização é preponderante analisar o que forças congéneres estão a fazer neste contexto, nomeadamente ao nível da União Europeia. Seria também interessante perceber a realidade da monitorização da internet e das redes sociais em sociedades orientais, como o Japão e a Coreia do Sul (E5).

3.9 Apresentação, análise e discussão da questão nº9

É determinante identificar e compreender as dificuldades a enfrentar na edificação desta capacidade por parte da GNR. É neste âmbito que surge a questão 9.

As restrições económicas surgem logo como uma das principais limitações, dado os gastos inerentes à formação e contratação de recursos humanos especializados, a compra de *software* automático e consequentes licenças de utilização (E5; E7).

Ao nível da prevenção criminal, outra das dificuldades sentidas prende-se com a dificuldade de criar e estabelecer *ciber-personas* totalmente desconetadas da instituição (E5; E6). Esta figura é essencial para aceder a grupos específicos que não estão acessíveis a todos os utilizadores das redes sociais, uma vez que a recolha e tratamentos de dados provenientes das redes sociais, não permite a utilização de meios intrusivos (E6).

Existe também uma limitação ao nível legal no que concerne à proteção de dados, uma vez que a retenção, tratamento de dados, ainda que públicos pode extravasar o campo do *profiling*, ou seja, a legitimação para analisar determinado perfil e/ou grupo (E7).

Ao nível das desvantagens, as redes sociais são altamente manipuláveis, através da automatização de perfis falsos e serviços de *clicking*. Esta manipulação pode não traduzir-se em resultados tangíveis no mundo real, o que pode levar a um policiamento mal dirigido e com resultados negativos (E7). A plataforma SENTINEL implementada em 2018 é um dos poucos casos em que esta preocupação foi dita em consideração aquando do seu desenvolvimento (Preece et al., 2018).

Este tipo de monitorização pode levar a uma perda de contato/proximidade com o cidadão no espaço físico e levar a uma consequente desvirtualização da função policial (E8).

3.10 Apresentação, análise e discussão da questão nº10

Tendo por base as limitações e desvantagens elencadas na questão anterior, pretendemos perceber quais os desafios a enfrentar na edificação desta capacidade por parte da GNR.

Um dos principais desafios a superar vai ser a falta de sensibilização para a importância das redes sociais na função policial, tanto ao nível dos operacionais, mas essencialmente ao nível da estrutura de comando, para a necessidade de investimento na monitorização policial das redes sociais (E5; E6;).

Diretamente relacionada com a necessidade de formação especializada, está a formação continua, por forma a manter os seus recursos humanos atualizados, bem como definir como será feita a gestão desses ativos (E6; E7).

A definição do seu enquadramento institucional, a sua missão e objetivos, bem como, a sua importância para a missão geral da GNR e para cada uma das suas missões especificas é essencial para definir um modelo de monitorização. Neste contexto específico é também importante perceber se deve ser uma atividade centralizada ou descentralizada (E7).

No âmbito da investigação criminal, um dos desafios passa por uma sensibilização da autoridade judiciária para a valoração da prova digital, recolhida no âmbito da monitorização das redes sociais. Perante esta necessidade é imprescindível um incremento da capacidade de resposta face às denúncias e atividades criminosas detetadas nas redes sociais (E8).

3.11 Apresentação, análise e discussão da questão nº11

Através das respostas a esta questão, pretendemos perceber de que forma a monitorização policial das redes sociais pode ter um papel preponderante na tomada de decisão e na manutenção da ordem pública e paz social.

Todos os inquiridos nesta questão revelam que a monitorização do discurso de ódio e a utilização de uma taxionomia que associa determinadas palavras a certos sentimentos com significado social pode ter uma associação empírica com a ocorrência de distúrbios de ordem pública e ocorrência de crimes, tanto no espaço físico, como no ciberespaço (E1; E2; E5; E6; E7; E8).

No entanto, é preciso perceber que o estudo destas duas variáveis ainda é muito recente e que é altamente volátil, uma vez que enfrenta vários fatores e elementos que podem adulterar a sua veracidade e utilidade. Uma das situações, que já foi referida anteriormente está diretamente relacionada com a utilização de dados manipulados propositadamente por *bootnets*[79] e serviços de *clicking* (E1). Outras das limitações prende-se com a partilha de conteúdos postados por perfis de famosos e que, na grande maioria dos casos, não corresponde à crença do utilizador que partilhou o *post*, ou simplesmente pode estar a ser irónico (E2). Como tal, esta monitorização tem de ser encarada como um complemento de outras atividades de recolha de informação e/ou atividades policiais (E7).

A monitorização eficiente destas duas variáveis permite perceber atempadamente quando um determinado foco de conflito ou uma tensão social poderá degenerar num distúrbio ou foco de conflito, pois tipicamente as redes sociais são utilizadas para ações de boicote ou manifestação (E7). Através de análise estatística sistemática, com recurso à elaboração de gráficos, é possível perceber estas tendências, com o objetivo de adotar medidas preventivas e reativas, facilitando assim a tomada de decisão e a manutenção da ordem pública (E5; E7; E8).

O discurso de ódio é hoje uma grande preocupação, com particular ênfase para a sua proliferação ao nível das redes sociais, uma vez que é conferido um elevado grau de anonimato aos utilizadores (E6; E7). Esta posição é também partilhada pela *Article 19*[80] (2015). De facto, existem cada vez mais projetos desenvolvidos nesta área por parte dos SMS e de outras associações para controlar esta problemática (E5).

---

[79] *Software* utilizado para criar perfis falsos e *post* com o intuito de transmitir desinformação.
[80] Associação ativista na área da liberdade de expressão.

3.12 Apresentação, análise e discussão da questão nº12

Através desta questão, pretendemos caracterizar a monitorização das redes sociais efetuada pela GC.

Na GC a monitorização das redes sociais é efetuado por todas as *jefaturas*[81] operacionais sob a dependência do *Mando de Operaciones Territoriales*, pese embora os meios técnicos e humanos mais sofisticados estarem alocados centralmente na *Jefatura deI informácion*[82] e *jefatura de policía judicial*[83], ambas sob a dependência do *Mando Información, investigatión y ciberdelincuencia* (E12, E13).

Em cada comunidade autónoma e, por sua vez em cada província, existe a capacidade de monitorização das redes sociais ao nível da *securidad ciudadana*[84]. Quando existe uma necessidade de monitorização ou de investigação criminal que extravase as capacidades da unidade territorial, ou que a situação em específico abarque uma criminalidade itinerante e complexa, a competência passa para as unidades centrais (E12; E13).

Como é impossível efetuar uma monitorização das redes sociais de modo permanente, a GC possui *software* sofisticado que permite recolher e analisar os dados de forma permanente das redes sociais, emitindo um aviso sempre que exista um sinal de alerta e/ou um desvio fora do padrão (E11). Dada a necessidade e as solicitações por parte dos analistas e operativos, existem subunidades que se dedicam ao desenvolvimento de ferramentas e *software* específico para a recolha e análise de dados e informação consoante cada situação específica (E11).

3.13 Apresentação, análise e discussão da questão nº13

Ao contrário da GNR, a GC detém a competência de investigação do cibercrime. Perante esta diferença, é importante perceber como estão organizados para fazer face a esta tipologia de criminalidade. Com esta questão pretende-se perceber o modo de atuação da GC relativamente ao cibercrime.

---

[81] Unidades.

[82] Responsável pela investigação e prevenção criminal de crimes contra o Estado (Terrorismo, Casa Real, ataques a infraestruturas criticas).

[83] Responsável peça investigação criminal do restante catálogo de crimes.

[84] Equivalente ao policiamento comunitário.

O combate e investigação do cibercrime e da criminalidade tecnológica não é considerado um crime contra o Estado, pelo que, a competência de investigação da GC é da *Jefatura de Policía Judicial* (E10).

Quando esta criminalidade se verifica a uma escala menor, é a *Unidad Orgánica de Policia Judicial* de cada comunidade autónoma ou a *Unidad de Policía Judiciaria* de cada província que é encarregue pela investigação. Estas duas unidades têm uma dependência técnica da unidade central: a *Jefatura de Policía Judicial*. A investigação passa para essa mesma unidade central quando existe um caso de extrema complexidade ou gravidade, e/ou quando se extravasa a competência técnica e territorial das unidades territoriais de *Policía Judicial*. (E10; E14).

A investigação esta adstrita a três subunidades diferentes. Na parte operativa temos a UCO; na parte de análise de informação criminal, relação e cooperação internacional está sob a alçada da UTP;, sendo a recolha de prova digital de meios técnicos a cargo do serviço de criminalística (E10).

A GC liga com mais casos de criminalidade tecnológica de cibercrime, sendo as redes sociais muito utilizadas como um meio de cometer burlas, ameaças e *bullyng* (E14). Uma das principais dificuldades sentidas na investigação destes crimes é a incapacidade de recolher prova com vista à identificação dos seus autores (E10).

3.14 Apresentação, análise e discussão da questão nº14

Nesta questão pretendemos caracterizar a utilização da SOCMINT por parte da GC, percebendo como é feita a sua recolha e análise.

A monitorização das redes sociais na GC visa essencialmente satisfazer a primeira fase do ciclo de produção de informações, ou seja, a recolha. Após a recolha, a informação é armazenada, sendo posteriormente analisada com vista à produção de relatórios de informações policiais. Para se efetuar esta análise é necessário relacionar a informação recolhida com outras fontes de informação (E11).

No caso concreto da SOCMINT é determinante selecionar o canal de informação adequado, uma vez que através de ferramentas de análise semântica é possível fazer uma análise com base em taxionomias e modelos comportamentais, que necessitam de ajuste consoante o contexto específico (E12). Dado este facto, torna-se impossível centrar esta monitorização, pois seria de todo impossível executar esta tarefa em todos os contextos simultaneamente (E12). Para se efetuar uma análise criteriosa é muito importante ter em

atenção dois aspetos, a taxionomia a utilizar e o potencial de difusão dos perfis estudados, e ter analistas especializados em áreas como a sociologia, que conhecem amplamente uma determinada realidade social. (E12).

No caso concreto da Catalunha a monitorização das redes sociais foi essencial, pois constituíram-se como os principais "veículos" de ativismo e *hacktivismo.* Depois de serem utilizadas para inflamar o espírito independentista, foi através destas plataformas que foram coordenadas as ações de manifestação e boicote a assembleias de voto, utilizando o *twitter,* bem como canais de *telegram* e *whattsapp* para o efeito. A coordenação era de tal maneira sofisticada que existia uma hierarquia na partilha da informação (E13). Ter perfis inseridos nestes canais foi determinante para evitar distúrbios civis de maior magnitude. Exercer este tipo de vigilância social nestas plataformas é a génese de da monitorização das redes sociais, devendo as FSS exercer aqui o seu esforço no que concerne a esta atividade, tal como previu Lyon (2001).

A utilização destas plataformas foi tão intensa que os analistas que trabalham na monitorização das redes sociais, em grande parte devido às *ciber-personas*, inseridas em canais de transmissão de mensagens instantâneas, perceberam primeiro a intenção dos manifestantes do que os militares e agentes no terreno, o que permitiu agir preventivamente em alguns casos (E13).

A situação vivida na Catalunha apresenta grandes semelhanças aos distúrbios em Vancouver (Trottier, 2012) e de Londres (Williams et al., 2013).

A utilização das redes sociais neste caso concreto entrou também no campo criminal, pois foram publicadas fotos e partilhada informação de pessoas que nutriam um sentimento nacionalista, por forma e exercer um controlo sob as mesmas (E13).

3.15 Apresentação, análise e discussão da questão nº15

Nesta questão pretende-se identificar e perceber quais as vantagens e desvantagens do modelo de policiamento adotado pela GC.

As redes sociais constituem-se como a principal fonte de recolha de informação, uma vez que são veículos utilizados para partilhar informação, que de outra forma as pessoas estariam inibidas de dizer diretamente às autoridades. A análise desta informação permite ter uma perceção daquilo que é realidade social, como não é possível em nenhuma outra plataforma. (E11; E12).

As redes sociais são utilizadas massivamente para orquestrar, organizar e planear atividades criminosas, pelo que a sua monitorização no âmbito policial permite identificar, compreender e prevenir o despoletar de fenómenos criminais latentes (E13).

No caso espanhol, através da sua atividade nas redes sociais, é possível identificar uma pessoa para efeitos judiciais, o que é uma grande vantagem da monitorização (E12).

Como principais desvantagens, temos a volatilidade associada a estas plataformas, dado que as redes sociais estão sempre em constante mudança, o que necessita uma capacidade de adaptação bastante elevada para manter uma monitorização permanente e contínua (E11).

Para além desta desvantagem, surge a questão económica, com a aquisição e manutenção de ferramentas técnicas, bem como, a formação e atualização de todos os recursos humanos (E11; E12; E13).

CONCLUSÕES E RECOMENDAÇÕES

Após o términus do trabalho de campo, que se concretizou na apresentação, análise e discussão dos resultados obtidos através das entrevistas, segue-se a última fase da investigação. Esta, que se materializa neste último capítulo, consiste em dar resposta às questões derivadas e à questão central que estiveram na origem da problemática. Este capítulo visa também apresentar uma reflexão sobre as potencialidades e limitações da investigação, bem como lançar o repto para trabalhos futuros ao apresentar algumas recomendações e sugestões.

Para dar resposta às questões derivadas, serão tidos em consideração todos os elementos reunidos na revisão da literatura, bem como na materialização do trabalho de campo.

Em resposta à QD1 "Como se caracteriza a monitorização policial das redes sociais?", esta atividade é um meio de observação da realidade social, uma vez que a função de segurança executada pelas FSS está amplamente dependente da sociedade em que está inserida. A sociedade portuguesa tem vindo a acompanhar aquilo que é a migração dos processos e interações sociais do espaço físico para o ciberespaço, com particular ênfase para as redes sociais. As sucessivas gerações estão cada vez mais dependentes da internet no seu modo de vida, o que leva a uma virtualização da vida social e, consequentemente, das FSS. Assim sendo, a missão primordial da GNR nas redes sociais é no âmbito das informações e prevenção criminal, exercendo uma atividade de vigilância, com o propósito de recolher dados que possam ser analisados e tratados.

Para que todo este processo de recolha, análise e tratamento seja feito de forma eficiente é necessário possuir um quadro técnico especializado, tanto para operar as ferramentas técnicas[85], como para correlacionar a informação obtida com um contexto social e/ou local, bem como com outras fontes. Dentro deste quadro técnico, especialistas da área da sociologia, teoria comportamental e estatística são fundamentais para se proceder a uma análise que traduza efetivamente a realidade social. Especialistas em programação informática são essenciais, uma vez que é necessário um constante

[85] Software de recolha e análise automática.

desenvolvimento e aperfeiçoamento das ferramentas técnicas de recolha e análise, consoante os pedidos dos analistas.

As redes sociais, na mesma medida que mudaram o paradigma de interação social, abriram também espaço para uma mudança na execução e preparação de atos ilícitos e criminais.

Perante este facto, os relatórios de informações policiais podem constituir uma ferramenta decisiva na prevenção criminal e manutenção da ordem pública, uma vez que estas plataformas são cada vez mais utilizadas para marcar, coordenar e executar ações de protesto que podem rapidamente transformar-se em distúrbios civis e perturbadores da paz social.

É também evidente que a monitorização policial das redes sociais pode conduzir a casos que constituam uma conduta criminosa. Entra-se então na esfera da investigação criminal.

Neste âmbito é fulcral estabelecer um canal de comunicação e partilha da informação com a autoridade judiciária, os ISP e os SMS. Os dados que se podem constituir como prova digital estão, na grande maioria dos casos, na posse destes operadores, pelo que a cooperação entre as autoridades e estes prestadores de serviços privados é essencial.

Importa referir que a informação recolhida das redes sociais necessita de ser conjugada com outras fontes OSINT e os operacionais no terreno, por forma a validar a mesma e conseguir uma perceção pormenorizada do ambiente operacional de um determinado evento, local ou contexto social.

Assim, a monitorização policial das redes sociais é vista como uma ferramenta complementar à missão da GNR, uma vez que permite auxiliar a atividade operacional na prevenção e investigação criminal, tanto no espaço físico como no ciberespaço.

Em resposta à QD2 "Em que espectro de atuação se insere a Monitorização das Redes Sociais da GNR?", presentemente o trabalho desenvolvido por esta força de segurança neste âmbito é bastante diminuto.

O incremento da capacidade ciber, com vista a garantir uma resposta integrada ao fenómeno da cibercriminalidade no espaço físico e virtual, é um dos objetivos estratégicos da GNR no horizonte 2020, tal como estabelecido no seu documento de orientação estratégica, "Estratégia da Guarda 2020". Volvidos três anos desde a sua publicação, esta capacidade pouco foi desenvolvida, uma vez que não existe qualquer orientação nesse

sentido. Um dos poucos resultados palpáveis foi o desenvolvimento de alguma literacia no âmbito da cibersegurança pelo grupo de trabalho constituído.

Eventualmente a falta de sensibilização da estrutura de comando para a importância desta problemática não permite desenvolver uma *Framework,* ou quadro organizacional, sob o qual esta capacidade seja desenvolvida. Sem estarem definidos os objetivos que se pretendem prosseguir com o incremento da capacidade ciber, não vai ser possível ter um desenvolvimento sustentado neste âmbito.

Como consequência desta situação, a monitorização das redes sociais desenvolvida pela GNR tem tido um contributo bastante diminuto para o cumprimento das missões que lhe estão atribuídas.

No que concerne à produção de informações policiais, tem sido desenvolvido algum trabalho pela Direção de Informações, sendo que a utilização da informação recolhida é feita de forma *ad-hoc,* conforme o caso em questão.

Esta situação ocorre devido à falta de meios técnicos, nomeadamente, a inexistência de um *software* automático de recolha e pesquisa de informação nas redes sociais. Associada a esta lacuna está a falta de recursos humanos, tanto em número como em formação. O efetivo adstrito a esta área é manifestamente insuficiente, para além da inexistência de um quadro de pessoal especializado em áreas fulcrais já identificadas.

Sem meios técnicos e pessoal especializado para analisar e interpretar a informação recolhida num contexto social e/ou local específico, o esforço de monitorização tornar-se-á infrutífero, uma vez que as informações policiais produzidas, a partir da informação recolhida nas redes sociais não têm validade para serem utilizadas como forma de perceção da realidade social.

Eventualmente este facto pode impossibilitar o seu emprego como ferramenta de apoio à tomada de decisão e manutenção da ordem pública, através da prevenção de distúrbios civis.

No que concerne à investigação criminal, já existe uma maior sensibilidade para a importância das redes sociais no desenrolar da investigação, sendo utilizadas bastantes vezes as notas práticas divulgadas pelo GCPGR, referente à cooperação internacional com os ISP e SMS, para recolha de *metadata* com vista a servir de prova digital.

Em resposta à QD3 "Que capacidades deve a GNR desenvolver e potenciar no âmbito da Monitorização Policial das redes sociais?", é necessário fazer uma conjugação entre a QD1 e QD2.

Antes de adquirir qualquer capacidade é necessário definir a já referida *Framework* organizacional, bem como os objetivos que se visa atingir com a monitorização das redes sociais.

No entanto, existe um conjunto de capacidades a desenvolver, tendo em vista tornar a monitorização das redes sociais eficiente, independentemente do seu âmbito de atuação e quadro organizacional. A mais importante de todas é adquirir um conjunto de especialistas, que possam analisar com propriedade a informação recolhida.

No que concerne ao equipamento técnico está em fase de processo de compra um *software* de recolha e análise automática de informação das *social media.* Este é já um passo muito importante dado pela GNR, por forma a dotar o CI desta capacidade. Ainda ao nível técnico é necessário começar a desenvolver *software* que permita identificar ações de discurso de ódio, para que através de um modelo taxionómico seja possível fazer associações entre palavras e sentimentos. Com este tipo de ferramentas é possível não só encetar ações de prevenção e sensibilização, como fazer um patrulhamento comunitário no ciberespaço.

Existe também a necessidade clara da importância das *ciber-personas* completamente desassociadas da instituição, que permitirá aceder a informação em grupos restritos, sendo na maioria dos casos é inacessível ao público em geral. A criação das referidas *ciber-personas* é uma medida técnica, mas que também necessita de um contexto de social e cultural específico, enfatizado a necessidade de um trabalho conjunto.

Um dos grandes problemas da informação recolhida das redes sociais é o seu grau de manipulação e baixo nível de verossemelhança entre aquilo que é publicado/partilhado pelo o utilizador e aquilo que este realmente pensa. De facto, existe muita desinformação na internet e nas redes sociais. Existem também muitos perfis com uma grande capacidade de difusão, nomeadamente personalidades famosas, o que leva a uma partilha excessiva dos conteúdos por si publicados. Quando falamos de *software* de recolha e análise automática, é necessário ter em consideração estes dois fatores, por forma a não atribuir qualquer grau de importância na produção de informações policiais.

Com vista a melhorar a formação e sensibilização para esta área, é necessário dotar os cursos bases com unidades curriculares desta temática, bem como uma aposta forte em formações de especialização ao nivel da OSINT, criminalidade tecnológica, cibercrime e cibersegurança.

No âmbito da investigação criminal o trabalho a desenvolver é junto da autoridade judiciária, dada a pouca valoração da prova digital recolhida no âmbito da monitorização das redes sociais nos inquéritos crime.

Perante o aumento do cibercrime e da utilização de meios tecnológicos na preparação e execução dos crimes tradicionais, a GNR tem de dotar a sua valência de investigação criminal com meios técnicos e formação adequada dos operativos, para proceder a uma recolha da prova digital a partir das redes sociais e garantir a sua cadeia de custódia.

No que respeita à QD4 "Como se caracteriza o modelo de Monitorização Policial das Redes Sociais desenvolvido pela *Guardia Civil?"*, importa referir que em relação à GNR é muito distinto, muito por força do contexto histórico e pela diferença de competência de investigação criminal[86].

A GC utiliza um modelo de monitorização descentralizado e global, ou seja, todas as *jefaturas* operacionais, ao nível central e territorial, exercem uma monitorização das redes sociais especificamente direcionado para as suas necessidades.

No entanto, as suas grandes capacidades nesta área estão adstritas às duas unidades de investigação criminal, a *Jefatura de Policía Judicial* e a *Jefatura de Informácion.* Esta última investiga crimes contra o Estado, nomeadamente, terrorismo, Família Real e ataques a estruturas críticas. Já a *Jefatura de Policía Judicial* investiga o restante catálogo de crimes, nos quais se insere o cibercrime e a criminalidade tecnológica. Neste contexto a investigação está divida em três unidades. A UTPJ é a unidade responsável pela análise de informação criminal, a UCO, unidade operativa que abarca para si os casos mais complexos das *Unidad Orgánica de Policía Judicial,* presentes em todas as comunidades autónomas espanholas e o laboratório forense digital do *Servivcio de Criminalistica*.

Como se pode perceber, o modelo de monitorização policial das redes sociais da GC está amplamente vocacionado para a investigação do cibercrime e criminalidade tecnológica, através da *Jefatura de Policía Judicial*, bem como, do ciberterrorismo e ataques a estruturas criticas, através da *jefatura de Informácion.* Estas duas unidades estão dotadas de um elevado numero de especialistas e capacidades técnicas, o que traduz em resultados práticos a sua atividade de monitorização.

[86] A GC tem competência de investigação criminal, que em muitos casos em Portugal é da reserva da PJ.

Ao nivel da *seguridade ciudadana*[87] a monitorização baseia-se essencialmente na vigilância social e georreferenciação das publicações.

A importância da monitorização das redes sociais no âmbito preditivo e preventivo de alterações da ordem pública, ficou bem patente durante a crise politica vivida na Catalunha. As redes sociais de mensagens instantâneas como o *whattsapp, telegram* e o *twitter,* foram utilizados como meios primordiais de comunicação, organização e coordenações das ações de protestos e disruptivas da paz social. Através de *ciber-personas* inseridas em grupos de conversação foi possível perceber antecipadamente, quais os locais que seriam alvo dos manifestantes, o que possibilitou orientar o esforço de policiamento, e com isso, ter uma ação preventiva ao invés de reativa, o que se revelou profícuo em bastantes casos.

A monitorização das redes sociais permitiu ter uma perceção sublime da dimensão e perigosidade dos protestos, ao contrário do *feedback* dado pelos militares no terreno.

Posto isto, estão então reunidas as condições para responder à QC "Que modelo de Monitorização Policial das Redes Sociais deve ser desenvolvido pela GNR?"

Primeiramente é importante estabelecer que não existem modelos de monitorização perfeitamente estabelecidos, pois as suas características variam bastante em função do contexto social, cultural e geográfico, bem como, do sistema de segurança interna em que estão inseridos.

No caso concreto da GNR e, tendo em conta as duas premissas anteriores, deve ser desenvolvido um modelo de monitorização policial das redes sociais como ferramenta complementar e de auxílio à atividade operacional, através da produção de informações policiais com vista à manutenção da ordem e tranquilidade pública, prevenção criminal e apoio à tomada de decisão.

Para cumprir esta tarefa é necessário definir os seus objetivos operacionais e uma *framework* organizacional, sendo que, tornar-se-ia imprescindível constituir uma equipa de especialistas em sociologia, teoria comportamental, estatística e engenharia informática, bem como adquirir um conjunto de ferramentas técnicas como *software* de recolha e análise de informação e a possibilidade de criação de *ciber-personas* descontextualizadas da realidade institucional.

Dado que os custos inerentes a edificar esta capacidade, este modelo deve ser centralizado, uma vez que não existe capacidade económica para o replicar ao nível

[87] Policiamento comunitário.

territorial, sendo a sua aplicabilidade prática também ela reduzida. Apesar a dispersão territorial da GNR, o CI dotado das capacidades suprarreferidas seria eventualmente capaz de fazer face às solicitações de monitorização e a fenómenos latentes pedidos pelas unidades territoriais.

As redes sociais servem como catalisador do cibercrime e criminalidade tecnológica, o que tem levado ao seu aumento exponencial. Assim sendo, a função de investigação criminal tem de ser desenvolvida neste modelo de monitorização policial das redes sociais. Uma resposta cabal por parte da GNR, nesta tipologia de crime, pode eventualmente contribuir para um aumento de inquéritos delegados nesta força de segurança.

De facto, as redes sociais são hoje o principal elemento da atividade social, onde uma única publicação tem um alcance tremendo, ao contrário daquilo que ocorre no espaço físico. A análise dessas publicações permite ter uma perceção da realidade social em que estamos inseridos. Perante este facto é possível perceber as necessidades de determinada população, o que permite orientar e dirigir o policiamento em virtude destas, bem como a difusão de informações nas mais variadas situações.

No entanto, é preciso sensibilizar para estas potencialidades, uma vez que não existe esta cultura no seio da instituição. Um esforço de formação e sensibilização dos militares neste sentido, é importantíssimo para a o sucesso deste modelo.

Nesta investigação, considera-se que o objetivo geral foi atingido através do cumprimento sequencial dos objetivos específicos, através da resposta às questões derivadas e questão central. Com base nas conclusões obtidas pretende-se enfatizar a importância e necessidade de se monitorizar as redes sociais no âmbito policial.

Uma das grandes limitações da investigação foi o facto de não poder assistir à monitorização de uma situação latente, pois permitiria uma análise qualitativa de uma situação concreta que certamente acrescentaria valor à investigação. Outras das limitações foi a impossibilidade de entrevistar responsáveis pelos gabinetes jurídicos das redes sociais.

Em futuras investigações sugere-se um estudo dedicado à importância da monitorização das redes sociais com impacto exclusivo do policiamento no ciberespaço.

Espera-se que este RCFTIA se constitua como uma mais-valia para a literacia institucional e uma ponte para investigações futuras.

BIBLIOGRAFIA

Academia Militar [AM] (2015). *Norma de Execução Permanente 520/4ª de 11 de maio: Trabalho de Investigação Aplicada.* Lisboa: Direção de Ensino.

Academia Militar [AM] (2016). *Norma de Execução Permanente 522/1.ª de 20 de janeiro: Normas para a redação de trabalhos de investigação.* Lisboa: Direção de Ensino.

Aghaei, S., Nematbakhsh, M. & Farsan, H. (2012). Evolution of The World Wide Web: From Web 1.0 to Web 4.0. *International Journal of Web & Semantic Technology.* 3-14.

Aires, L. (2011). *Paradigma Qualitativo e Práticas de Investigação Educacional.* Lisboa: Universidade Aberta.

Alves, A. C. (2008). *Em Busca de uma Sociologia da Polícia.* Lisboa: Revista da Guarda Nacional Republicana.

Alves, A. C. (2010). *Introdução à Segurança* . Lisboa: Revista da Guarda Nacional Republicana.

Amaral, L. (1994). *Planeamento de Sistemas de Informação.* Tese de Doutoramento, Universidade do Minho, Braga.

Article 19 [A19] (2015). *"Hate Speech" Explained.* Londres: Article 19 Publisher.

Ascensão, J. O. (2001). *Estudos Sobre Direito da Internet e Sociedade e Informação.* Lisboa: Almedina.

Assembleia da República [AR] (2008). Lei nº 49/2008 de 27 de agosto: Lei da Organização da Investigação Criminal. *Diário da República*, 1.ª Série, nº 165, 6038-6042.

Assembleia da República [AR] (2009). Lei nº 109/2009 de 15 de setembro: Lei do Cibercrime. *Diário da República*, 1.ª Série, nº 179, 6319-6325.

Assembleia da República [AR] (2014). Lei nº 4/2004 de 13 de agosto: Lei Quadro do Sistema de Informações da República Portuguesa. *Diário da República*, 1.ª Série, nº 155, 4194-4206.

Assembleia Geral das Nações Unidas [AG-ONU] (1966). Convenção Internacional dos Direitos Civis e Politicos. *Sistema de Documentação Oficial das Nações Unidas*. Vol. I - 14668.

Association of Chief Police Officers [ACPO] (2000). *Manual of Guidance on Keeping the Peace.* Bramshill: National Police Trainning Center.

Barrinha, A. & Carrapiço, H. (2016). Cibersegurança. In R. Duque, D. Noivo & T. Silva (Edits.), *Segurança Contemporânea* (pp. 245-262). Lisboa: Pactor.

Berg, B. L. (2001). *Qualitative Research Method for the Social Sciences* (4ª ed.). California: Allyn & Bacon.

Berners-Lee, T. & Cailliau, R. (1990). WorldWideWeb: Proposal for a HyperText Project. In *W3C*. Acedido a 21 de abril de 2018 em *https://www.w3.org/Proposal.html.*

Betz, D., & Stevens, T. (2012). *Cyberspace and the State: Toward a Strategy for Cyber-Power.* Londres: Routledge.

Branco, C. (2010). *Guarda Nacional Republicana - Contradições e Ambiguidades.* Lisboa: Edições Silabo.

Burnap, P., Williams, M., Morgan, J. & Housley, W. (2014). *Working paper 153: Social Media Analysis, Twitter and the London Olympics*. Cardiff: University of Cardiff. Acedido a 13 de abril de 2018 em *http://www.cardiff.ac.uk/socsi/research/publications.*

Caldas, A. (2011). Uma Estratégia Nacional de Cibersegurança. (P. Noguês, Ed.) *Segurança & Defesa*. 94-98.

Caldas, A. & Freire, V. (2013). *Cibersegurança: das Preocupações à Ação*. Lisboa: Instituto da Defesa Nacional.

Castells, M. (1996). *The rise of the network society (The information age: Economy, Society and Culture) (Vol. 1(1)).* Oxford: Blackwell Publishers, Inc.

Chainey, S. (2008). Identifying priority neighbourhoods using vulnerable localities index. *Policing*. 2(2), 106-209.

Choudhury, N. (2014). World Wide Web and Its Journey from Web 1.0 to Web 4.0. *International Journal of Computer Science and Information Technologies*. 5, 22-27.

Clark , D., Leiner , B., Cerf, V., Kahn, R., Kleinrock, L., Lynch, D. & Roberts, L. (1997). *Internet Society*. Acedido a 10 de março de 2018 em *https://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf.*

Clemente, P. (2010). Polícia e Segurança. *Politica Internacional e Segurança*. 141-171.

Clemente, P. (2008). *As informações de Polícia - Palimpsesto.* Lição Inaugural do Ano Académico 2008/09. Lisboa: Instituto de Ciências Policiais e Segurança Interna.

Community Oriented Policing Services & Police Executive Research Forum [COPS; PERF] (2013). *Social Media and Tactical Considerations For Law Enforcement*. Washington DC: COPS/PERF.

Conselho Europeu [CE] (2001). *Convenção Sobre o Cibercrime.* Budapeste: Conselho Europeu.

Conselho Europeu [CE] (2010). Estratégia de Segurança Interna da União Europeia. In *Portal do Conselho Europeu.* Acedido a 4 de abril de 2018 em *http://www.consilium.europa.eu/media/30754/qc3010313ptc.pdf.*

Coutinho, V. (2014). *The Social Book: Tudo o que precisa de saber sobre o Facebook.* Lisboa: Actual Editora.

Cruz, M. J. (2015). *Guardar Portugal: Qual o papel da GNR.* Lisboa: bnomics.

Dias, P. (2014). *Viver na Sociedade Digital: Tecnologias Digitais, Novas Práticas e Mudanças Sociais* (1ª ed.). Cascais: Princípia.

European Police Office [EUROPOL]. (2016). Internet Organised Crime Threat Assessment (IOCTA). In *Portal Europol*. Acedido a 2 de maio de 2018 em *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-c rime-threat-assessment-iocta-2016.*

Europeia, C. (2007). *Rumo a uma Política Geral de Luta Contra o Cibercrime.* Bruxelas: União Europeia.

Fernandes, A. J. (2010). *Introdução à Ciência Política: Teorias, Métodos e Temáticas* (3ª ed.). Porto: Porto Editora.

Flick, U. (2005). *Métodos Qualitativos na Investigação Científica* (1ª ed.). Lisboa: Moniotr.

Fortin, M. F. (2009). *O Processo de Investigação: da concepção à realização* (5ª ed.). Loures: Lusociência.

Freixo, M. J. (2012). *Metodologia Cientifica: Fundamentos, Métodos e Técnicas.* Lisboa: Instituto Piaget.

Fuchs, C. (2008). Internet and Society: Social Theory and Self-Organization. *Systemic Practice and Action Research.* 16(4), 113-167.

Ghosh, S. & Turrini, E. (2010). *Cybercrimes: A Multidisciplinary Analysis.* Nova Iorque: Springer.

Giddens, A. (1999). *O Mundo na Era da Globalização* (1ª Edição ed.). Lisboa: Editorial Presença.

Giddens, A. & Sutton, P. (2013). *Sociology.* Cambridge: Polity Press.

Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Social* . São Paulo: Atlas.

Guarda Nacional Republicana [GNR] (2014). Estratégia da Guarda 2020. In *Portal da Guarda Nacional Republicana*. Acedido em 15 de abril de 2018 em *http://www.gnr.pt/InstrumentosGestao/estrategia_2020.pdf.*

Guerra, I. C. (2006). *Pesquisa Qualitativa e Análise de Conteúdo - Sentidos e Formas de Uso* (1ª ed.). Estoril: Princípia.

Held, D., McGrew, A., Goldblatt, D. & Perraton, J. (1999). *Global Transformations: Politics, Economics, and Culture.* Stanford: Stanford University Press.

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services [HMIC] (2011). *The rules of engagement: A review of the August 2011 disorders.* Londres: HMIC.

Internation Telecommunication Union [ITU] (2009). *Overview of cybersecurity.* Genebra: ITU Publisher.

Ji, Y., Hwangbo, H., Ji, S., Rau, P., Fang , X. & Ling, C. (06 de novembro de 2010). The Influence of Cultural Differences on the Use of Social Network Services and the Formation of Social Capital. *International Journal of Human-Computer Interaction*. 26:11-12, 1100-1121.

Kaplan, A. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*. 59-68.

Kaspersky Laboratories (2018). What is Cyber-Security? In *Kaspersky Lab*. Acedido a 29 de março de 2018 em *https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.*

Kauark, F., Manhães, F. & Medeiros, C. (2010). *Fundamento de Pesquisa: Um Guia Prático* (5ª ed.). Bahia: Via Litterarum.

King, M. & Waddington, D. (2004). Coping with disorder? The changing relationship between police public order strategy and practice - a critical analysis of the Burnley Riot. *Policing and Society*. 14(2), 118-137.

Kozlovski, N. (2007). A Paradigm Shift in Online Policing - Designing Accountable Online Policing. In J. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman & T. Zarsky (Edits.), *Cybercrime. Digital Cops and Laws in a Networked Environment* (pp. 107-134). Nova Iorque: New York University Press.

Lourenço, N., Lopes, F., Rodrigues, C., Costa, A. & Silvério, P. (2015). *Segurança Horizonte 2025 - Um Conceito Estratégico de Segurança Interna.* Lisboa: Edições Colibri.

Lyon, D. (2001). *The Surveillance Society - Monitoring Everyday Life.* Buckingham: Open University Press.

Marconi, M. & Lakatos, E. (2003). *Fundamentos de metodologia cientifica* (5ª ed.). São Paulo: Atlas.

Marques, G. & Martins, L. (2006). *Direito da Informática* (2ª ed.). Coimbra: Almedina.

Militão, R. L. (2013). Ordem dos Advogados. In *Portal da Ordem dos Advogados*. Acedido a 23 de março de 2018 em *http://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf.*

Moleirinho, P. E. (2009). *Da Polícia de Proximidade ao Policiamento Orientado pela Informações.* Dissertação de Mestrado, Mestrado em Direito e Segurança, Universidade Nova de Lisboa, Lisboa.

Newburn, T. (2011). *Handbook of Policing* (2ª ed.). Nova Iorque: Taylor & Francis.

O'Reilly, T. (2005). Design Patterns and Business Models for the Next Generation of Software. In *O´Reilly*. Acedido a 11 de março de 2018 em *http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1.*

Parzlale, L., Britt, D., Davis, C., Forrester, J., Llu, W., Matthews, C. & Nicolas, R. (2006). International Business Machines. In *International Business Machines*. Acedido a 9 de março de 2018 em *http://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf.*

Pereira, C. Q. (2013). *Análise Criminal e Sistemas de Informação.* Trabalho de Investigação Individual do CEM-C, Instituto de Estudos Superiores Militares, Pedrouços.

Ponsaers, P. (2001). Reading about "Community (Oriented) Policing" and Police Models. *Policing: An Internation Journal of Police Strategies & Management*. 24(4), 470-497.

Postman, J. (2008). *SocialCorp: Social Media Goes Corporate* (1ª ed.). Berkley: New Riders Press.

Preece, A., Spasic, I., Evans, K., Rogers, D., Webberley, W., Roberts, C. & Innes, M. (2018). Sentinel: A Codesigned Platform for Semantic Enrichment of Social Media Streams. *IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS*. 5(1), 118-131.

Procuradoria-Geral da República [PGR] (2017). *Relatório da Atividade setembro 2015 – dezembro 2016*. Lisboa: Gabinete do Cibercrime da PGR.

Quivy, R. & Campenhoudt, L. V. (2013). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Ramalho, D. S. (2017). *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina.

Ring, C. (2013). *Hate Speech in Social Media: An Exploration of the Problem and its Proposed Solutions.* Univerty of Colorado, Journalism & Mass Comunication. Boulder: Univerty of Colorado.

Robinson, N., Gribbon, L., Horvath, V. & Robertsion, K. (2003). *Rand Corportation.* Acedido a 29 de março de 2018 em *https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.*

Rodrigues, B. S. (2009). *Direito Penal - Parte Especial - Tomo I - Direito Penal Informático-Digital.* Coimbra: Coimbra Editora.

Santos, D. (2014). *A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança*. Lisboa: ISCTE - Instituto Universitário de Lisboa.

Sarmento, M. (2013). *Guia Prático sobre Metodologia Científica para a ELaboração Escrita e Apresentação de Teses de Doutoramento.* Lisboa: Universidade Lusíada Editora.

Schneider, J. & Trottier, D. (2012). The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing. *BC Studies.* 175, 57-72.

Simas, D. (2014). *O Cibercrime*. Lisboa: Universidade Lusófona.

Singer, P. & Friedman, A. (2014). *Cybersecurity and Cyberwar.* Nova Iorque: Oxford University Press.

Sistema de Segurança Interna [SSI] (2017). *Relatório Anual de Segurança Interna – 2016.* Lisboa: SSI.

Strate, L. (1999). The varietis of cyberspace: Problems in definition and delimitation. *Western Journal of comunication.* 63(3), 382-412.

Torres, J. (2005). A Investigação Criminal na PSP. *Estratégia de Gestão Policial em Portugal*. 579-636.

Trottier, D. (2012). Policing Social Media. *Canadian Review of sociology.* 49 (4), 411-425.

United States Army [USA]. (2010). *FM 3-19-50 Police Intelligence Operations.* Washington DC: Department of The Army.

Vaz, A. (2015). As Informações Policiais. *Revista de Direito e Segurança.* 5, 39-55.

Venâncio, P. D. (2011). *Lei do Cibercrime Anotada e Comentada* (1ª ed.). Coimbra: Coimbra Editora.

Verdelho, P. (2005). Cibercrime e Segurança Informática. *Policia e Justiça - Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais*. 159-175.

Viegas, J. M. (1998). *Direitos humanos e eficácia policial. Sistemas de controlo da atividade policial, [Acta das intervenções do seminário internacional]*. Lisboa: IGAI.

Waters, M. (1999). *Globalização.* Oeiras: Celta Editora.

Williams, M., Edwards, A., Housley, W., Burnap, P., Rana, O. & Sloan, L. (2013). Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing & Society*. 23(4), 461-481.

APÊNDICES

APÊNDICE A - CARTA DE APRESENTAÇÃO E GUIÃO DA ENTREVISTA

ACADEMIA MILITAR

Direção de Ensino

Mestrado em Ciências Militares na Especialidade de Segurança

TRABALHO DE INVESTIGAÇÃO APLICADA

Contributo para um Modelo de Monitorização Policial das Redes Sociais pela Guarda Nacional Republicana

Autor: Aspirante Aluno de Infantaria da GNR João Carlos de Almeida Canatário

Orientador: Professor Doutor José Fontes

Coorientador: Major de Infantaria da GNR Pedro Miguel Ferreira da Silva Nogueira

Relatório Científico Final do Trabalho de Investigação Aplicada Lisboa, março de 2018

CARTA DE APRESENTAÇÃO

A Academia Militar (AM) é um estabelecimento de ensino superior público universitário militar com a finalidade principal de formar Oficiais destinados aos quadros permanentes do exército e da Guarda Nacional Republicana (GNR).

Tendo em vista à obtenção do grau, os alunos redigem um Trabalho de Investigação Aplicada (TIA), sendo este submetido à apreciação e discussão pública perante um júri, cujo o objetivo, em contexto de investigação, passa pela execução das competências adquiridas, o desenvolvimento de capacidades e exposição das suas conclusões.

Desta forma, venho por este meio solicitar a V. Ex.ª a colaboração no âmbito do TIA, dada a necessidade de realização de entrevistas tendo em vista a recolha de informações, bem como, o esclarecimento de questões diretamente ligadas à investigação, subordinada ao tema: "*Contributo para um Modelo de Monitorização Policial das Redes Sociais pela GNR"*.

Esta investigação tem como objetivo geral perceber de que forma o modelo de policiamento das redes sociais a adotar pela Forças e Serviços de Segurança, em particular pela GNR, pode evitar alterações do estado de ordem pública. Para tal definiram-se dois vetores para atingir esse objetivo: a *CyberIntelligence* tendo por base informações referentes a indicadores de tensão e "discurso de ódio*";* bem como, a investigação e o combate aos vários tipos de cibercriminalidade perpetrada através das Redes Sociais.

Grato pela colaboração e disponibilidade.

Atenciosamente,

João Carlos de Almeida Canatário

Aspirante

GUIÃO DE ENTREVISTA

Contributo para um Modelo de Monitorização Policial das Redes Sociais pela Guarda Nacional Republicana

1. IDENTIFICAÇÃO DO(A) ENTREVISTADO(A)

1.1. Nome:	1.6. Idade:
1.2. Organização/Órgão:	1.7. Habilitações literárias:
1.3. Departamento/Serviço:	1.8. Local:
1.4. Cargo/Posto:	1.9. Data-Hora (início/fim):
1.5. Função:	

2. ENQUADRAMENTO

No âmbito do TIA, submetido ao tema: *"Contributo para um Modelo de Monitorização Policial das Redes Sociais pela GNR"*, tendo em vista a obtenção do grau de Mestre em Ciências Militares, na especialidade de Segurança, conferido pela Academia Militar, emerge a presente entrevista, a fim de esclarecer questões decorrentes da investigação e aprofundar os conhecimentos adquiridos, aplicando-os no contexto operacional da GNR e das FSS.

A rápida propagação das plataformas de *Social Media* criou novas formas para as pessoas interagirem e partilharem informação, tornando-se amplamente reconhecido que as referidas plataformas são uma fonte de informação valiosa, com carácter operacional e de apoio à tomada de decisão. Esta mudança de paradigma trás consigo tanto benefícios como riscos para a sociedade, bem como novos desafios para as instituições de segurança, nomeadamente, as Forças e Serviços de Segurança.

É então que surge a necessidade de um modelo de monitorização nas redes sociais, capaz de correlacionar a análise de padrões de identificação, de comportamento, e de associação que permite uma análise de risco abrangente e unificada.

Esta investigação tem como objetivo geral perceber como se caracteriza e qual o âmbito da monitorização policial nas redes sociais por parte das Forças e Serviços de Segurança, especificamente o da Guarda Nacional Republicana (GNR).

Pretende-se analisar a atuação ao nível da recolha de informações das redes sociais (OSINT & SOCMINT), no que concerne a manifestações de tensão social, nomeadamente, *Hate-Speech e CyberProtesting*. bem como, a atuação referente à prevenção, combate, e investigação do cibercrime perpetrado através das redes sociais.

Esta investigação conta também com uma análise comparativa com o modelo de monitorização das redes sociais da *Guardia Civil*, dada a proximidade naquilo que é a realidade social e cultural espanhola e portuguesa, e na diferença de competências entre as duas Forças de Segurança, nos referentes Sistemas de Segurança Interna.

3. ENTREVISTA

1. Qual é o quadro de atuação das Forças e Serviços de Segurança no âmbito do Monitorização nas Redes Sociais?

2. Considera ser, a Monitorização das Redes Sociais, um instrumento importante na prevenção e combate à criminalidade? Em que medida?

3. No âmbito da Monitorização das Redes Sociais, a troca de informação entre as empresas gestoras de serviços de internet, de redes sociais e as autoridades judiciárias, é preponderante. Deste modo, como funciona este processo e quais as principais dificuldades?

4. Sob que âmbito, e quais as medidas implementadas nesse sentido, tem a GNR baseado a sua Monitorização das Redes Sociais?

5. De que forma contribui a Monitorização das Redes Sociais para o cumprimento das missões da GNR?

6. No âmbito das informações, em que medida pode a SOCMINT constituir-se como um instrumento de medida de indicadores de tensão social? Qual a atuação da GNR neste sentido?

7. Tendo em conta o quadro legal vigente qual é a atuação da GNR, perante os vários tipos de cibercrime perpetrados nas redes sociais?

8. Considerando o espectro de atuação da GNR, que capacidades se devem desenvolver no âmbito da Monitorização nas Redes Sociais?

9. Quais as limitações e desvantagens da Monitorização das Redes Sociais efetuado pela GNR?

10. Considerando as atuais limitações e desvantagens, que desafios se impõem à atividade de Monitorização?

11. Em que medida, pode a monitorização do discurso de ódio e da taxionomia de sentimentos,

constituir-se, como uma ferramenta de apoio à decisão e de ordem pública?

APÊNDICE B - RELAÇÃO DAS QUESTÕES DE INVESTIGAÇÃO COM O GUIÃO DE ENTREVISTA

Quadro 1 - Quadro Relação das Questões de Investigação e o Guião da Entrevista

Objetivos de Investigação	Questões de Investigação	Questões Entrevista
OG: Analisar quais as características, capacidades e âmbito de atuação de um modelo de Monitorização Policial das Redes Sociais por parte da GNR	**QC:** Que modelo de Monitorização Policial das Redes Sociais deve ser desenvolvido pela GNR?	
OE1: Caracterizar a Monitorização nas Redes Sociais no âmbito da atividade Policial	**QD1:** Como se caracteriza a Monitorização Policial das Redes Sociais	**1)** Qual é o quadro de atuação das Forças e Serviços de Segurança no âmbito da Monitorização das Redes Sociais? **2)** Considera ser, a Monitorização Policial das Redes Sociais, um instrumento importante na prevenção e combate à criminalidade? Em que medida? **3)** A Troca de informação entre as empresas gestoras de serviços de internet, de redes sociais e as autoridades judiciárias, é preponderante. Como funciona este processo e quais as principais dificuldades?
OE2: Identificar o espectro de atuação da GNR na Monitorização das Redes Sociais	**QD2**: Em que espectro de atuação se insere a Monitorização Policial das Redes Sociais da GNR?	**4)** Sob que âmbito, e quais as medidas implementadas neste sentido, tem a GNR baseado a sua Monitorização das Redes Sociais? **5)** De que forma contribui a Monitorização das Redes Sociais para o cumprimento das missões da GNR? **6)** No âmbito das informações, em que medida pode a SOCMINT constituir-se como um instrumento de medida de indicadores de tensão social? Qual a atuação da GNR neste sentido? **7)** Tendo em conta o quadro legal vigente qual é a atuação da GNR, perante os vários tipos de cibercrime perpetrados nas redes sociais?

OE3: Identificar as capacidades a desenvolver e as limitações a mitigar por parte da GNR na Monitorização das Redes Sociais	**QD3:** Que capacidades deve a GNR desenvolver e potenciar no âmbito da Monitorização Policial das redes sociais?	**8)** Considerando o espectro de atuação da GNR, que capacidades devem ser desenvolvidas no âmbito da Monitorização Policial das Redes Sociais? **9)** Quais as limitações e desvantagens da Monitorização Policial das Redes Sociais efetuada pela GNR? **10)** Considerando as atuais limitações e desvantagens, que desafios se impõem à atividade de Monitorização? **11)** Em que medida, pode a monitorização do discurso de ódio e da taxionomia de sentimentos, constituir-se, como uma ferramenta de apoio à decisão e ordem pública?
OE4: Caracterizar a atuação da *Guardia Civil* na Monitorização Policial das Redes Sociais	**QD4:** Como se caracteriza o modelo de Monitorização Policial das Redes Sociais desenvolvido pela *Guardia Civil*?	**12)** Sob que âmbito, e quais as medidas implementadas nesse sentido, tem a *Guardia Civil* baseado a sua Monitorização Policial das Redes Sociais? **13)** Como e caracteriza o modo de atuação da *Guardia Civil* relativamente ao cibercrime? **14)** Como se caracteriza o modelo de recolha de tratamento da SOCMINT por parte da *Guardia Civil?* **15)** Quais as vantagens e desvantagens/restrições do modelo de Monitorização Policial das Redes Sociais da Guardia Civil

Fonte: Autor

APÊNDICE C - LISTAGEM DOS ENTREVISTADOS

Quadro 2 - Lista de Entrevistados

Grupo Entrevistados	Entrevistados	Questões	Função/cargo	Data e Local
Grupo 1	Professor Doutor Martin Innes – E1	Questões 1/2/3/6/11	Diretor do *Crime and Security Research Institute – University of Cardiff*	Via Skype em 23/04/2018
	Professor Doutor Daniel Trottier – E2		Professor Associado Universidade de Roterdão	Via Skype em 11/04/2018
Grupo 2	Procurador da República Pedro Verdelho[88] – E3	Questões 1/2/3/7	Coordenador do Gabinete do Cibercrime da Procuradoria-Geral da República	22/04/2018 - Lisboa
	Inspetor Coordenador Carlos Cabreiro – E4		Diretor da Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica da PJ	13/04/2018 – UNC3T Lisboa
Grupo 3	Tenente-Coronel Carlos Pimentel - E5	Questões 1 a 11	Ex membro do Grupo de Trabalho de Cibersegurança da GNR	09/04/2018 – ANPC Carnaxide
	Tenente-Coronel Paulo Machado – E6		Chefe da Divisão de Estudos e Análise de Informação Criminal da GNR.	13/04/2018 – DIC Alcabideche
	Major Rogério Raposo – E7		Coordenador do Departamento de Operações do Centro Nacional Cibersegurança	11/04/2018 – Belém
	Major Adriano Rocha – E8		Chefe do Centro de Informações da DI/CO	05-04-2018 – EG

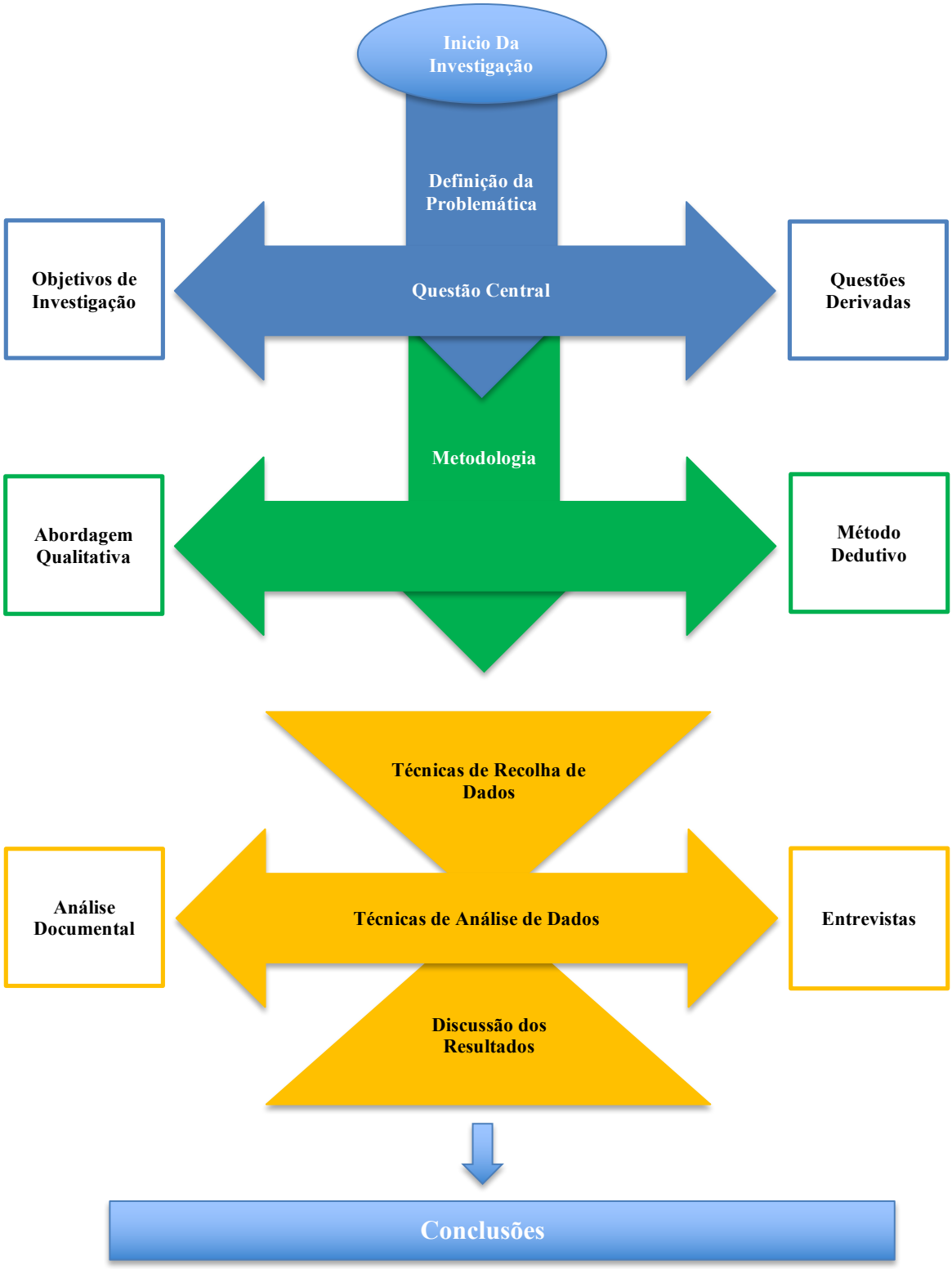
[88] Por opção não responde à pergunta 7.

	Capitão Raquel Valente – E9[89]		Responsável pela gestão das páginas Institucionais da GNR nas redes sociais - DCRP	03/05/2018 - Lisboa
Grupo 4	Tenente António Bautista[90] – E10	Questões 12 a 15	*Jefe de Sección del Grupo de Ciberdelincuencia*[91] - *Unidad Técnica de Polícia Judicial – Jefatura de Polícia Judicial - Guardia Civil*	16/04/2018 – UTPJ Madrid
	Comandante (Major) José Mayorga Martín – E11		*Comandante Jefe del Área Técnica – Jefatura de Información – Guardia Civil*	17/04/2018 – *Jefatura de Information* Madrid
	Tenente Enrique Martín Aláez – E12		*Jefe de Sección del Grupo de Ciberterrorismo – Jefatura de Información – Guardia Civil*	17/04/2018 – *Jefatura de Information* Madrid
	Tenente José Luís – E13		*Jefe de Sección del Grupo de Ciberterrorismo – Jefatura de Información – Guardia Civil*	17/04/2018 – *Jefatura de Information* Madrid
	Oficial Unidad Central Operativa[92] (UCO) – E14[93]		*Unidad Central Operativa (UCO) – Grupo de Delitos Telemáticos*	18/04/2018 – UCO Madrid

Fonte: Autor

[89] Dada a missão que desempenha na GNR apenas responde às questões 1,2 e 7, no âmbito exclusivo da comunicação.
[90] Sendo um especialista na área do cibercrime, desempenhado funções exclusivas neste âmbito na GC apenas responde à questão 13.
[91] Em Português significa Cibercrime.
[92] Sendo um especialista na área do cibercrime, desempenhado funções exclusivas neste âmbito na GC apenas responde à questão 13.
[93] Por razões de confidencialidade não será revelada a sua identidade.

APÊNDICE D - DESENHO DE ESTUDO



Fonte: Autor

APÊNDICE E - ANÁLISE QUALITATIVA DE RESULTADOS

Quadro 3 - Sinopse das respostas à questão de entrevista n.º 1

Nº	Resposta	Sinopse
E1	**"**Não tenho a certeza se a estrutura de monitorização policial está contruída e tem a estrutura certa (...) As decisões do que priorizar e o que tem precedência são essenciais"	- "(...) A organização e o pensamento estratégico das policias tende a ser estruturado através da tradicional organização de unidades e departamentos." "(...) o meu trabalho procura investigar e comparar como a monitorização das redes sociais e a sua análise está a ser utilizada nas funções de investigação, e informações no âmbito do crime organizado, ordem pública e policiamento comunitário (...) descobrimos que está a ser utilizado com muito sucesso quando utilizado de maneira competente. No entanto, é utilizado muitas vezes de forma ingénua".
E2	**"**Estas ferramentas de monitorização não vão resolver os problemas sozinhas. Podem providenciar informação importante, mas que necessita de um contexto local e social	- **"**De certa forma não difere de outras atividades realizadas pelas FSS. No âmbito de criminal tem de atuar da mesma maneira que o faz no mundo físico, pois tem de prevenir e investigar práticas criminais" "Numa perspetiva de OSINT pode fornecer informação importante e em maior quantidade do que qualquer fonte de OSINT." - "No âmbito da comunicação, as FSS têm de perceber o contexto social, local e das suas atribuições, para perceber o que é que a comunidade em que estão inseridos necessita em termos de comunicação externa por parte das autoridades policiais. "
E3	"(...) não tem sido feito, de forma regular ou organizada qualquer monitorização das redes sociais"	- "Ao nível da prevenção criminal, tanto quanto sei não existe de forma regular ou organizada qualquer policiamento das redes sociais. O acesso, no contexto de investigações, tem sido reativo: embora com exceções em geral, apenas se acede a redes sociais para procurar informação de crimes que já ocorreram."
E4	"A agregação de dados recolhidos através da monitorização das redes sociais pode efetivamente tornar-se uma ferramenta de prevenção criminal e perceção da realidade social"	- **"**É evidente que as redes se constituem como um veiculo para a prática de crimes, não para o crime informático propriamente dito, mas sim para os crimes cometidos com recurso a meio informático. Este facto não é mais do que uma transposição dos crimes antigos do meio físico para uma nova plataforma que é a internet, e que as redes sociais vieram potenciar (...)" - "Existe verdadeiramente uma necessidade neste sentido, pois as redes sociais constituem-se como um novo espaço de atuação do cidadão. Se as FSS tiverem uma visão conjugada e uma análise da atividade dos cidadãos nestas plataformas, decerto que essa informação será valiosíssima em termos de informações policiais no âmbito criminal, quer na perspetiva da prevenção, quer na parte preditiva, através da atuação propriamente dita nas redes sociais e também na própria investigação."
E5	"(...) pode trazer um conjunto de informações (...) que podem levar a uma orientação, seja ela no âmbito da *CyberIntelligence,* ou de cariz criminal."	- "A monitorização das redes sociais pode trazer um conjunto de informações, que trabalhados de uma maneira coerente e organizada, através de um conjunto de ferramentas e procedimentos, podem levar a uma orientação, seja ela no âmbito da *CyberIntelligence*, ou no de cariz criminal." - "Hoje em dia cada vez mais as pessoas partilharam os seus estados de alma nas redes sociais, pelo que, é importante termos a capacidade de "medir o pulso" da sociedade para que estejamos alerta para alguns fenómenos sociais."
E6	"(...) o principal quadro de atuação das FSS na monitorização das redes sociais é de facto a prevenção criminal"	- "Esta monitorização terá de ser sempre efetuada no quadro das atribuições de cada FSS. No caso da GNR, designadamente no âmbito das suas atribuições de prevenção e investigação criminal. No caso de um inquérito crime que esteja a decorrer, em função dos suspeitos, pode existir a necessidade da recolha de prova através da monitorização das redes sociais"
E7	"Sempre numa perspetiva de prevenção, eventualmente de alerta ou pré-prevenção, através de uma atuação pró-ativa	- "Medir a tensão social para poder prever um possível incidente ou um ciberataque, é algo que também está diretamente ligado às redes sociais." -"Um exemplo concreto é o 25 de abril, 10 de junho, 25 de novembro e dias de eleições. Nestas datas o ativismo acaba por ter um pico de atividade perfeitamente visível através das redes sociais." - "Utilização de técnicas de *marketing massivo e* estruturar as mesmas para a atividade policial"

E8	"A monitorização das redes sociais visa primordialmente a obtenção de informações. (...)Obtenção de informações de segurança e/ou Informações policiais e criminais (...)	- "Informações de Segurança: desenvolvidas por serviços públicos de informações (...) ou seja, pelo SIED e SIS e que visam ser preventivas e prospetivas. (...) a monitorização de informação nas redes sociais visa a produção de informações de segurança" - "Informações policiais e criminais: Desenvolvidas pelos OPC de competência genérica e especifica (LOIC). (...) os de competência genérica (GNR, PSP, PJ) para além das informações criminais, desenvolvem as informações policias, as quais têm como fim último a obtenção de informação de ordem pública."
E9	"(...) comunicação entre a instituição e as pessoas, assumindo-se de certa forma como um importante instrumento de marketing e comunicação institucional."	- "Sendo a GNR uma instituição vocacionada para as pessoas (...) tem de estar onde as pessoas estão. Atendendo que um grande número de pessoas está nas Redes Sociais, também a GNR aqui marca presença, nomeadamente no *Facebook*, no *Twitter*, no *Instagram* e no *YouTube*. Assim, o quadro de atuação da DCRP nas redes sociais é no âmbito da comunicação, sendo esta missão, dentro da Divisão, desenvolvida pela Repartição de Comunicação" - "No que se refere à monitorização, dentro do quadro de atuação da DCRP, esta é numa ótica de ajuste de estratégias de comunicação nestas plataformas, por forma a determinar o sentimento das pessoas relativamente à instituição, nomeadamente quais os interesses dos nossos seguidores e quais os temas do momento, por forma a tornar a nossa comunicação mais eficiente e eficaz."

Fonte: Autor

Quadro 4 - Sinopse das respostas à questão de entrevista n.º 2

Nº	Resposta	Sinopse
E1	"Pode ser uma ferramenta muito poderosa quando associado a outras fontes de informação, através de técnicas de fusão e associação"	- "Os casos mais convincentes que observei envolvem a capacidade de enriquecer o quadro de atuação da policia sobre o crime e distúrbios de ordem pública." - "É também útil na identificação de crimes de baixa visibilidade em termos da sua prevalência e distribuição geográfica. Apesar disso assumo o meu ceticismo sobre algumas das alegações que são feitas sobre o facto de ser utilizado para prever padrões e tendências criminais. "
E2	"Muitos dos aspetos da vida social estão associados às redes sociais, e, portanto, a monitorização é essencial na prevenção e combate à criminalidade."	- "Dada a migração dos aspetos da vida social para as redes sociais, é inquestionável a importância das ferramentas de monitorização das redes sociais na prevenção e combate à criminalidade." - "(...) o *software* pode recolher a informação, no entanto, a sua análise requer um contexto local e social. O próprio *Software* necessita de ser programado de uma maneira específica que o ligue às necessidades de informação relacionadas com a especificidade de um evento, área ou população."
E3	**"**Sem dúvida que o é: as redes sociais têm permitido perceber que há fenómenos criminais que estas redes potenciam"	- **"**Acedendo as redes sociais, as autoridades podem prever acontecimentos em planeamento. As redes facilitam a conjugação de esforços entre os vários interventores em planos criminosos e, aperceber estas conjugações, permitiria evitar crimes. Além disso, mesmo sem aludir a crimes, há criminosos que estão presentes nas redes. Acompanhar a sua prestação nestas redes permitiria seguir o seu percurso e, não só evitar a prática de crimes como, além disso, mais facilmente investigar aqueles crimes que, entretanto, lograssem praticar.
E4	"têm de se posicionar naquilo que é esta nova realidade digital da internet e das redes sociais"	- "É evidente que as forças policiais no âmbito da prevenção criminal têm de se posicionar naquilo que é esta nova realidade digital da internet e das redes sociais" "(...)até na própria investigação a monitorização se torna importante, dado que grande parte dos dados inerentes à prova acabam por estar nas redes sociais e nas comunicações que acabam por estar subjacentes a estas."
E5	"(...) aperceber das suas tendências. (...) pode-se orientar o policiamento, por forma a prevenir uma atividade ilícita (...)"	- "Se monitorizarmos as redes sociais de uma forma continua, e também através da nossa presença, vamos começar a aperceber das suas tendências." - "É necessário criar um conjunto de *ciber-personas*, que não estejam identificadas com a instituição, através de mecanismos diversos, que encaixem nos perfis de determinados grupos destinados a atividades ilícitas. Isto é fazer o policiamento de acordo com as informações, através de um atitude mais pró-ativa do que reativa."
E6	"(...) é muito importante esta monitorização, pois vai concorrer para as atribuições da guarda na prevenção e na investigação."	- "Cada vez mais se verifica uma migração de alguns fenómenos do meio físico para o mundo virtual (ciberespaço). Um exemplo prático desta situação no âmbito da investigação criminal, eram as reuniões que antigamente sucediam num espaço público, que exigiam muitas vezes um relatório de diligência externo no âmbito de um inquérito, e que neste momento ocorrem no ciberespaço, com particular incidência para as redes sociais. Situação semelhança acontece com as manifestações ou distúrbios civis, ou seja, neste momento o agendamento e

		coordenação destas atividades são efetuadas em fóruns na internet, como são exemplos típicos os CTT ou encerramentos de centro de saúde, balcões da CGD ou centro escolares."
E7	"É um instrumento importante para preservar a paz social, ou pelo menos perceber que atividades podem perturbar a mesma (...) complementa aquilo é a atividade policial"	- "É mais um fator que integra na formula de combate à criminalidade, podendo dar uma maior precisão daquilo que é a missão geral da GNR (...) através de economia de meios, otimização do policiamento (...), o que, tudo integrado dará uma atuação mais eficiente. - "Policiamento direcionado para os problemas específicos, independentemente do policiamento genérico que será sempre importante. Capacidade extra de direcionar o patrulhamento em função das informações recolhidas."
E8	"Nas redes sociais, pode-se obter informação policial criminal (...) a informação daí extraída poderá em muito canalizar e auxiliar na atividade preventiva e repressiva das FSS (...)"	- "Atualmente existem vários estudos que indicam que entre os 80% e os 90% da informação policial e criminal pode ser obtida em fontes abertas (open sources)." "(...) pode-se obter a imensa informação policial e criminal, tais como eventuais agendamentos de ações de protesto, conflitos entre grupos, transações ilícitas de bens, venda ilegal de bens, burlas" - "(...) a qual tem como fim último a manutenção da ordem e tranquilidades pública"
E9	"(...) São uma importante ferramenta de prevenção."	- "Dentro Do quadro de atuação da DCRP, consideramos que as Redes Sociais são uma importante ferramenta de prevenção. Por isto mesmo, utilizamos as nossas páginas para difundir diversos conselhos de segurança, com o objetivo de alertar os nossos seguidores para os comportamentos que devem adotar para evitarem ser vítimas de crimes."

Fonte: Autor

Quadro 5 - Sinopse das respostas à questão de entrevista n.º 3

Nº	Resposta	Sinopse
E1	**"**Esta troca de informação é umas das principais dificuldades sentidas"	- "No futuro veremos que o comportamento coletivo na internet exigirá uma combinação de policiamento e regulamentação, que neste momento não acontece, uma vez que os princípios que definem a policia enquanto instituição social simplesmente não se adaptam no ciberespaço"
E2	**"**Os ISP e os SMS estão geralmente noutros países diferentes daqueles em que o MP requer os *metadata,* o que levanta uma questão legal"	- **"**Para além da questão legal, as próprias empresas têm alguns interesses a defender, nomeadamente os dados pessoais dos seus utilizadores." - "É, portanto, crucial estabelecer um mecanismo de cooperação por forma a facilitar a partilha de informação entre atores públicos e privados. Este mecanismo não invalida a necessidade de análise consoante os casos por parte dos referidos atores."
E3	**"**Foram estabelecido protocolos de cooperação com alguns destes operadores"	- **"**O gabinete do cibercrime desenvolveu protocolos de cooperação judiciária, que em alguns casos permite um contato direto entre as partes. Para esclarecer estas situação foram desenvolvidas notas práticas (...) que foram divulgadas a todas as FSS (...)"
E4	"Tanto no âmbito da prevenção como do combate e investigação à criminalidade, tem de se atuar junto dos referidos operadores, uma vez que, são eles que detém muita da informação referente à atividade desenvolvida nestas plataformas e que é essencial para constituir prova."	- "O processo de cooperação que existe no âmbito policial que tem a sua materialização nos inquéritos crime passa por uma atuação institucional, e muitas das vezes judicial, através do juiz de investigação criminal. Esta relação de cooperação tem de estar muito bem articulada, pois, tem de se saber muito bem a informação que se pede aos operadores, tendo sempre em mente, que a grande parte dos mesmos é estrangeiro, e por isso é necessário percorrer o circuito da cooperação internacional." - "A cooperação entre as partes existe sem sombra de duvidas. No entanto, o que pode acontecer por vezes é esta não ter a celeridade exigida para que produza efeito. A necessidade da informação pode perder o seu efeito se esta não for obtida em tempo útil, o que, em criminalidade tecnológica acaba por ter um peso muito maior do que nos demais tipos de crime." - "Em termos policiais é bastante importante os pontos de contato 24/7, e deve ser neste que se deve de investir e desenvolver mecanismos de cooperação mais célere e consequentemente mais eficientes."
E5	**"**(...) no caso dos ISP com a legislação europeia em vigor, estes mecanismos devem ficar segundo um	- "No caso dos ISP, a própria legislação já obriga a uma retenção de dados. Com a entrada do *General Data Protection Regulation* (GDPR), um cenário alterou um bocado" - "Cada uma destas empresas até pela sua obrigação está obrigada a ter um órgão

	padrão de cooperação e partilha de informação com as autoridades judiciárias.	responsável por ser um ponto de contato, bem como, a figura responsável por implementar um conjunto de medidas previstas na lei. (Custódio de Segurança). Isto tem um impacto direto nos dados que os OPC podem recolher e integrar em processos judiciais, por forma a se tornarem prova." - "Na parte dos utilizadores que estão inseridos numa rede corporativa, essa mesma rede pode ter um conjunto de regras que permitem registar e reter os *metadata*. "
E6	**"**A Procuradoria-Geral da República, através do Gabinete do Cibercrime difundiu notas práticas sobre esta temática."	- **"**No caso da investigação criminal, esta informação já foi remetida tecnicamente a toda a sua estrutura. Ou seja, todos os militares que fazem parte da referida estrutura, sabem como proceder no que concerne a este tipo de diligências no âmbito de um inquérito, pois este caso específico aplica-se mais no caso da investigação criminal do que da prevenção." - "Nas notas práticas estão descritos todos os procedimentos, e que de facto agilizam bastante todo o processo e as operadoras retém logo os dados pedidos por parte da autoridade judiciária."
E7	"(...) atuarem no espaço europeu ficam sob jurisdição da União Europeia (...) tudo o que se faz no digital deixa um rastro, por isso, esta colaboração acaba por ser muito importante "	- "Apesar De muitos dos servidores não estarem alojados na União Europeia, pelo simples facto de estes provedores de serviços de redes sociais e de internet a atuarem no espaço europeu, ficam sob jurisdição da legislação europeia, nomeadamente, no caso específico dos regulamentos de proteção de dados." - "Neste âmbito a PJ acaba por ter canais de comunicação privilegiados em virtude dos seus pontos de contato permanente, seja diretamente ou através da Interpol ou Europol (...) a continuar a colaborar para criar mecanismo de cooperação (...) depende da União Europeia e da postura das empresas"
E8	"As empresas gestoras de serviços de internet e de redes sociais têm outros objetivos e politicas que estão muito longe dos objetivos das entidades policiais"	- **"**De facto, a partilha de informação e conhecimentos entre estas entidades deveriam de ser efetivo" - "(...)a autoridade judiciária nem sempre está sensibilizada para a importância e manancial de informação vital que se pode extrair das redes sociais e do que a partir daí se pode garantir para a fim último da manutenção da ordem e tranquilidades pública."

Fonte: Autor

Quadro 6 - Sinopse das respostas à questão de entrevista n.º 4

Nº	Resposta	Sinopse
E5	"Neste momento a GNR não desenvolve grande atividade nesta área. (...) a monitorização feita é muito ad-hoc"	- "O grande pontapé de saída neste âmbito será dado quando se adquirir o software necessário, e através da formação tanto dos analistas como dos operativos. Neste âmbito sei que está a ser criado o primeiro curso OSINT na GNR, mas até lá, está apenas a fazer-se um levantamento das necessidades. (...) existe, no entanto, a consciência da necessidade de criar *ciber-personas*"
E6	"Ao nível da prevenção é quando ocorrem fenómenos latentes, e nestes casos a monitorização pode ser feita central ou localmente"	- "Ao nível central estão a ser desenvolvidas capacidades ao nível do futuro CI da GNR (...) da parte da prevenção não existe grande trabalho na área, no entanto, num futuro próximo e através do CI pode dar-se um salto qualitativo neste âmbito." - **"**De referir que é impossível manter uma monitorização a 100% e 24h por dia das redes sociais, no entanto é bastante importante esta atividade em determinados fenómenos para efeitos de prevenção criminal, como é o caso dos discursos de ódio."
E8	"A GNR apresenta ainda um reduzido numero de produtos face àquilo que se perspetiva para o futuro"	- "(...) decorre da Estratégia 2020. No âmbito deste documento, foi definido uma reestruturação da Direção de Informações, sendo que no decurso da mesma foi identificada a necessidade do levantamento da capacidade OSINT" - "(...) para que esta capacidade esteja edificada na sua totalidade, carece ainda da aquisição de software OSINT automático bem como da alocação e formação de recursos humanos (...) na constituição do CI/DI/CO."

Fonte: Autor

Quadro 7 - Sinopse das respostas à questão de entrevista n.º 5

Nº	Resposta	Sinopse
E5	"Contribui imensamente para a missão da GNR. A verdade é que hoje em dia quase tudo se passa nas redes sociais"	- "Temos como exemplo os maus tratos a animais que agora estão em voga, nos quais existe um grande ativismo através das redes sociais. Nesse sentido é essencial a GNR estar presente nestas plataformas, estando disponível para receber comunicação (denúncias – Canal direto via Comando-Geral), como também recolher a informação que nos permite planear e melhor organização as várias operações."
E6	**"**É essencialmente no âmbito das missões de vigilância (...)"	- "Uma das atribuições da GNR, é garantir a segurança e o exercício dos DLG, o que leva a uma necessidade de prevenir a criminalidade em geral tanto no meio físico como no ciberespaço." - "Se durante esta atividade de monitorização se constatar a prática de crimes mesmo que manifestamente infundados o OPC tem obrigatoriamente de comunicar ao MP (...)"
E7	**"**Ferramenta de apoio e (...) complementar à missão geral da GNR"	- "(...) Produção de informações, apoio à investigação criminal, ajuda no processo de decisão, e manutenção da tranquilidade pública e paz social." - "(...) no mundo físico passou para o virtual (..) o que pode levar a uma decisão errada, visto que, a ação no ciberespaço pode não corresponder necessariamente a uma ação no espaço físico. Perante esta problemática é necessário atribuir um grau de verossemelhança a determinada informação, em função do seu valor policial."
E8	"(...) a valência ainda se encontra em edificação, pelo que o seu contributo ainda é reduzido"	- "Contudo o que se pretende no futuro é que esta valência por um lado, pesquise e recolha informações policiais que oriente o policiamento e auxilie na tomada de decisão do Comando e, por outro, obtenha informação criminal que auxilie as investigações criminais em curso (remetidas à DIC/CO)."

Fonte: Autor

Quadro 8 - Sinopse das respostas à questão de entrevista n.º 6

Nº	Resposta	Sinopse
E1	"Pode ser bastante útil para monitorizar tensões sociais, no entanto, tem de ser utilizado com bastante cuidado"	- "Eu utilizo mais o conceito de *Open Source Communications*, como uma forma de recolha e análise da componente essencial das redes sociais, a sua qualidade de diálogo, ou seja, o incentivo de interações e trocas de informação entre os seus utilizadores" - "É, no entanto, necessário ter cuidado, uma vez que, existem atores que devido a um leque de motivações acabam por inflamar deliberadamente os níveis de tensão social, através de *boots*. A forma como se deve responder a este tipo de comportamento ainda não está bem definido."
E2	"(...) os indicadores sociais requerem um conhecimento local e social"	- "As origens do acesso e análise a indicadores sociais tem as suas origens no setor do *marketing*. Aplicar estas ferramentas num contexto policial necessitaria de uma adaptação do *software,* o que por si só abarca limitações à sua implementação" "(...) toda a informação recolhida necessita necessariamente de uma confirmação ao nível local"
E5	"(...) o verdadeiro desafio é escolher os indicadores a monitorizar (...) pois, as redes sociais, são elementos de expressão da realidade social(...) especialistas da sociologia e da teoria comportamental (...)	- "Depois de selecionados os indiciadores, basta seguir as suas variações e quais as tendências que vão seguindo, através de ferramentas estatísticas." - "(...)para se escolherem bons indicadores, é preciso estar presente no meio em questão ou por dentro da problemática que se visa estudar. Para se fazer uma boa escolha, só através da experiência, de uma correta perceção, ou através da experiência de terceiros, pela sua literacia, que permite desenhar um padrão e consequentemente perceber as tendências. Aqui a análise do trabalho desenvolvido por congéneres é essencial, bem como, perceber qual a sua aplicabilidade à realidade social portuguesa." - "Aqui o essencial não se prende com a tecnologia empregue, mas com a análise do contexto que se pretende analisar por parte de peritos."
E6	**"**(...) o conceito de SOCMINT tem de ser densificado e mais trabalhado, pois umas das suas principais atribuições será a ordem pública"	- "E através de ferramentas de SOCMINT podemos constatar se localmente determinados fenómenos de ordem pública se estão a manifestar, ou seja, temos de nos preparar para atuar preventivamente para garantir a segurança dos cidadãos**."** - "(...) uma situação latente (...) pode levar à ocorrência de cortes de estradas, agressões e distúrbios da ordem pública. Assim, a monitorização das redes sociais pode tornar-se um instrumento de vigilância bastante efetivo deste tipo de

		manifestações. Neste particular a monitorização tem de se basear na prevenção.”
E7	**“**Tem de ser algo que tem de ser medido e afinado constantemente, ser redundante. Necessita de um pensamento estruturado.”	- **“** Os níveis de tensão social necessitam de pressupostos base: 1- O que é que se procura nas redes sociais e que peso lhes vou dar (em função da verossemelhança de quem praticou o ato e o seu contexto)” 2- Quem produz o comentário (...) e qual a sua capacidade 3- Tecnicamente passa por perceber que as fontes de OSINT mudam a sua tecnologia, o que implica uma constante adaptação”
E8	“(...) tomada de decisão (...) prevenção da ordem e tranquilidades públicas”	- “Através das redes sociais e de software automático com a aplicação de taxonomias é possível obter informação sobre sentimentalismos/intenções podendo dessa forma auxiliar na prevenção da ordem e tranquilidades públicas, bem como na orientação do policiamento e auxílio da tomada de decisão (...)”

Fonte: Autor

Quadro 9 - Sinopse das respostas à questão de entrevista n.º 7

Nº	Resposta	Sinopse
E4	“Este tipo de criminalidade assolou-nos de uma forma muito rápido e ainda não houve uma reação ao nível legislativo para se fazer face a esta realidade.” “Na criminalidade informática ou com recurso a meio informático existem duas situações (...) se é um ato isolado, ou se concerne a um fenómeno criminoso, com um alto nível de organização (...)”	-**“**A evolução diz nos que a prática de crimes com recurso a meio informático está a aumentar exponencialmente, o que, vem deixar de parte a necessidade de especialização que existia no passado, e que colocava alguns entraves na investigação deste tipo de criminalidade. É evidente que a generalização da utilização da internet e o próprio uso da tecnologia informática também generalizou a necessidade de investigação. Perante esta premissa, terá necessariamente de se arranjar um outro tipo de critério, de forma, a perceber quando é que um crime praticado com recurso a meios informáticos é passível de ser investigado pela GNR ou PSP. Tem igualmente de se perceber em que situações em que o mais importante é o fenómeno, a realidade organizada do crime, ou apenas um ato isolado. É algo para o qual, terá efetivamente de se refletir e adaptar a LOIC nesse sentido, pois terá de ser percebido que atualmente, grande parte da criminalidade tem um meio informático envolvido, seja como instrumento ou alvo.
E5	“Perante os crimes conduzido através de meios informáticos tem uma clara competência, até porque, vai ser esta, a maior área de trabalho da GNR”	- “De facto, não existe praticamente nenhum crime cometido em que não exista um meio informático envolvido, e neste âmbito concreto, o *whattsapp* é um claro exemplo desta realidade, pois a criminalidade exige sempre um tipo de comunicação instantânea.” - “No caso do cibercrime em sentido estrito, dada a competência reservada da PJ, a atuação da GNR prende-se quase em exclusivo com as medidas cautelares e de policia. Ainda assim, dado o crescimento deste tipo de criminalidade e a sua dinâmica, esta realidade por vir a ser alterada. “ - “Aqui é essencial a instituição adquirir literacia nesta temática, pois cada vez mais as pessoas que recorrem a estas áreas são de faixas etárias maiores, que por natureza não estão despertas para os perigos que enfrentam no ciberespaço.”
E6	“A utilização de um meio digital nos crimes em que a GNR é competente para investigar, não invalida enquanto OPC a sua competência de investigação”	- **“**Está a assistir-se a uma migração dos crimes do meio físico para o digital, o que leva a que, de uma forma ou de outra, a grande maioria dos crimes hoje perpetrados levem a uma utilização do meio informático” “Aquilo que é da competência reservada da PJ são os crimes previstos na Lei do Cibercrime. De acordo com a LOIC, no seu artigo 8º, mesmo estes crimes podem ser delegados num outro OPC que não a PJ, desde que se afigure mais adequado em concreto ao bom andamento da investigação.”
E7	“O MP decide a quem delega a condução da investigação (...), no entanto, o mais importante é garantir o principio do sucesso da investigação e que se atinja o objetivo da mesma, em detrimento dos órgãos que a investigam.	- “A LOIC atribui competência reservada nesta matéria à PJ, que inclui todos os tipos de cibercrime, seja os previstos na Lei do Cibercrime, como também aqueles em que meio informático, é o “inicio, meio ou fim” do crime. Ou seja, pode ser o meio para a realização de um crime e/ou o objeto do mesmo. Isto não invalida que a GNR tenha esta competência, e como tal, os meios e o conhecimento para investigar.” - “Se existe uma competência deve ser respeitada e acautelada, o que não invalidade a complementaridade dos OPC. Se existir capacidade em conduzir uma boa investigação em matéria de cibercrime e onde a cadeia de custódia da prova seja acautelada, concordo que qualquer OPC possa ter a competência de investigar um cibercrime de qualquer natureza”
E8	“(...) verifica-se é a utilização do meio	- “(...) pese embora o cibercrime em sentido lato ser da competência reservada da PJ, tendo em consideração que numa grande maioria das tipologias criminais

	informático para realização do crime e não do cibercrime (...) abre-se assim a janela para atuação da GNR e PSP"	aquilo que se verifica é a utilização do meio para a realização do crime e não o cibercrime" - "Nesse âmbito o trabalho que decorre na GNR assenta na monitorização das diferentes fontes abertas, sendo que aquando da deteção de informação criminal, a mesma após tratada é remetida à DIC/CO, para autuação e instrução do processo."
E9	"(...) a DCRP divulga conselhos de segurança aos seguidores (...) situações que possam consubstanciar crime (...) sejam devidamente analisadas"	- "Dentro desta temática, a DCRP divulga conselhos de segurança aos seguidores, para que estes adotem comportamentos preventivos. Por outro lado, sempre que nos divulgam, através de mensagens privadas ou comentários, situações que possam consubstanciar crime, a DCRP reencaminha-as para o Comando Operacional, para que as mesmas sejam devidamente analisadas e, caso se aplique, sejam tomadas medidas."

Fonte: Autor

Quadro 10 - Sinopse das respostas à questão de entrevista n.º 8

Nº	Resposta	Sinopse
E5	"É essencial uma sensibilização nos cursos base (...) é preciso dotar as pessoas que vão trabalhar nesta área de competências especificas."	- "(...) será necessário observar o que fazem as outras forças de segurança no estrangeiro, nomeadamente na União Europeia. Neste contexto seria importante analisar o contexto de sociedades orientais como o Japão e da Coreia do Sul, pois no seu contexto social as redes sociais têm um peso enorme. Inclusivamente, a grande maioria dos processos socias são efetuados através destas plataformas, existindo cada vez mais uma dificuldade nos processos sociais cara-a-cara." - "Apesar se se dar uma grande importância à sensibilização, é igualmente importante a especialização dos militares que trabalhem nesta área, quer em ciências socias, quer em estatística."
E6	"(...) no caso da investigação (...) formar os militares desta estrutura naquilo que é a prova digital (...) nomeadamente na transcrição de serviços de troca de mensagens instantâneas"	"Falando apenas no caso da investigação, existe um esforço de formação em todos os cursos de investigação criminal, no sentido de formar os militares desta estrutura naquilo que é a prova digital, nomeadamente como se pode recolher a prova na internet, garantido a sua cadeia de custódia, bem como, sensibilizar os militares para este novo meio de prova." "(...) ao nível do investigador operativo para estar devidamente habilitado a fazer a recolha da prova digital e garantir a sua cadeia de custódia no âmbito da prova" "Apesar de a DI e a DIC serem direções diferentes, estão ambas subordinadas ao CO. Se de facto durante a sua atividade de vigilância e pesquisa a DI detetar um crime, já está definido um canal de comunicação com a DIC para proceder às diligências de que está incumbida."
E7	"(...) tem de se ter um objetivo muito bem definido (...) de acordo com a missão geral e estratégia da GNR." "Perceber em que é que a monitorização contribui para uma atividade especifica"	"(...) desenvolver uma *Framewrofk (*Quadro Organizacional). Definir a sua dependência orgânica e funcional (...). Tem de ser provido de recursos, tendo por base o objetivo que se precisa de atingir. Ter um quadro de pessoal de áreas especializadas (...) como por exemplo sociólogos (...) que têm uma grande capacidade de trabalhar sobre grandes volumes de dados, fazendo agregações e consequentemente conclusões importantes (...) o que implica perceber a informação que se vai recolher para se conseguir processar (...) analisar e interpretar"
E8	"(...)Tendo em conta o manancial de informação que se pode obter (...) urge alocar recursos humanos e dotá-los tecnicamente (...)"	"A GNR tem de ter em consideração que a monitorização requer recursos humanos técnicos, que por vezes demora anos a constituir-se como um perito e a dominar as diferentes ferramentas, com especial destaque, para as ferramentas manuais OSINT"

Fonte: Autor

Quadro 11 - Sinopse das respostas à questão de entrevista n.º 9

Nº	Resposta	Sinopse
E5	"(...) económica, seja para dar formação, comprar equipamento ou estudar outras realidades."	"Limitações: As redes sociais são muito de modas- Para perceber as suas tendências é necessário estar presente nestas plataformas. Aqui é essencial focar-se no ambiente de estudo. (...) a falta de meios tecnológicos não permite a criação de *ciber-personas*." "Desvantagens: Necessidade de uma grande formação dos recursos humanos"
E6	"(...) ter um perfil de utilizador completamente desconectado da instituição, o que se torna muito difícil em temos práticos"	"(...) no âmbito de prevenção criminal não existe lugar à utilização de meios intrusivos, pelo que, a atuação passa pela mera observação. Ou seja, acaba por ser uma analogia com a patrulhamento dos militares no espaço físico, que também estão em observação da atividade social, estando também restritos na utilização de meios intrusivos" "(...) ao nível da prevenção (...) tem de se ter um perfil completamente desconectado da instituição (...).
E7	"(...) limitações legais (...) Deslumbramento pelos resultados (...) Ir por resultados falsos entre a rede social e o mundo civil (...) Manter a formação e os recursos humanos atualizados"	"(...)ver se o contexto na altura da monitorização legitima esta atividade, e se não extravasa para o campo do *Profiling*. "Pode levar ao um desligamento no mundo físico. É muito fácil monopolizar uma rede social, através da automatização de comentários, criar perfis falsos, entre outros serviços de *clicking*, o que não se traduz em resultados tangíveis no mundo real." "Ir por falsos resultados entre as redes sociais e o mundo civil. pode levar a um policiamento mal dirigido e influenciado."
E8	"Dificuldade de identificação de autores. (...) Desvirtualização da função policial."	- "Perda do contato/proximidade com o cidadão. " - "Dificuldade de identificação dos autores aquando do cometimento de atividades ilegais." - "Desvirtualização da função policial."

Fonte: Autor

Quadro 12 - Sinopse das respostas à questão de entrevista n.º 10

Nº	Resposta	Sinopse
E5	"Falta de sensibilização (...)"	"Falta de sensibilização dos profissionais desta área, mas essencialmente, da estrutura de comando para a importância desta problemática."
E6	"(...) formação e sensibilização dos militares que vão trabalhar neste âmbito de monitorização"	"A formação tem que ser continua de forma a acompanhar a perante evolução nas redes sociais e a sensibilização tem que ser constante junto dos militares. Depois de estas premissas estarem adquiridas é que se pode pensar nas ferramentas técnicas como é o caso do *software.*"
E7	"O enquadramento funcional e organizacional desta atividade. Definir competências (...) Manter a formação atualizada"	"(...)definir as suas dependências, quais os seus objetivos, que informações vai produzir, em que âmbito, qual o seu intuito e que peso terá na missão geral, e em cada uma das missões especificas da GNR. Importa também saber a sua descentralização ou não." "Definir as competências das pessoas que vão desempenhar funções, e de que forma será feita a sua gestão e (...) manter a formação atualizada"
E8	"(...) Sensibilização da autoridade judiciária (...) Incremento de capacidade"	- "Sensibilização e enquadramento da autoridade judiciária para junção da informação obtida como prova." - "Reformulação do conceito de policiamento da GNR" - "Incremento da capacidade de resposta face às denuncias e atividades ilícitas detetadas em meio ciber".

Fonte: Autor

Quadro 13 - Sinopse das respostas à questão de entrevista n.º 11

Nº	Resposta	Sinopse
E1	"Sim, efetivamente pode ser utilizado, mas necessita algum cuidado, uma vez que ainda não se percebeu como estas variáveis se associam."	- **"**Na pesquisa que conduzimos associado ao projeto OSCAR, em alguns casos identificamos uma associação empírica entre o discurso de ódio online e a ocorrência de crimes quer no espaço físico quer no ciberespaço." - "No entanto, noutros caso essa associação acaba por não estar presente. Para além desta falta de associação existem um conjunto de complexidades relativas à desinformação, uma vez que os dados online são facilmente manipulados, o que pode influenciar o comportamento coletivo"
E2	"Ferramentas que detetam o discurso de ódio trazem óbvios benefícios em principio, mas acarreta algumas limitações no que concerne à sua veracidade e pró-atividade"	- "(...) é extremamente difícil ver se os dados não se tratam de uma partilha ou se o utilizador não está a ser irónico. As dificuldades sentidas neste âmbito são enfatizadas pelo enorme volume de dados que a monitorização pode providenciar, mesmo com a ajuda de *software*." - "Os perfis com muitos seguidores têm um papel vital neste âmbito, uma vez que as *trends* que partilham são muitas vezes partilhados pelos seus seguidores, o que, em muitos casos, podem não corresponder às suas crenças." "Isto, pode equivocar a atividade policial, senão existir uma cooperação com a policia local, para verificar os indicadores localmente."
E5	"(...) Quantificação deve ser tomada em atenção (...) Começar a redirecionar o policiamento, por forma a reduzir ao máximo as tensões" (...) mais do que as ferramentas (...) é importante selecionar os indicadores adequados."	- No contexto de um evento social, um conjunto de pessoas começam a referir-se a este de uma forma inflamada, tendo no seu discurso um conjunto de palavras que já foram identificadas como sendo indiciadoras de padrões comportamentais de distúrbios, (...) uma ferramenta que nos ajuda à "customização social portuguesa", seria bastante importante para se poder pelo menos, (...) redirecionar o policiamento, por forma a reduzir ao máximo as tensões. - ".No entanto, a grande maioria desta atividade desenvolve-se em grupos fechados, como os Hooligans, o que enfatiza a necessidade de ter ciber-peronas integradas num determinado contexto específico."
E6	"Muito importante, principalmente a nível do discurso de ódio que constitui uma grande preocupação a nível europeu	- "A FRA e a OCDE têm grupos de trabalho permanentes para fazer face ao discurso de ódio, e existem projetos piloto que visam monitorizar as redes sociais." - "A GNR está a efetuar ações de prevenção de crimes de ódio, num trabalho conjunto com a APAV e DGPJ"
E7	"Constitui uma ferramenta de apoio à decisão e da paz social, pois garante uma atuação preventiva. Dá uma capacidade pró-ativa (...) serve de complemento de outras atividades de recolha de informação e/ou atividade policial."	- "Dá uma capacidade pró-ativa quando é percebido atempadamente que pode surgir um determinado foco de conflito ou uma tensão social que irá degenerar num distúrbio, pois, tipicamente as redes sociais são utilizadas para ações de boicote ou manifestação. É algo que não deve ser encarado fora da missão geral da GNR, ou seja, esta monitorização serve como complemento de outras atividades de recolha de informação e/ou de atividade policial." - "Tipicamente as redes sociais são o palco discurso de ódio, dado o anonimato conferido aos comentadores. O anonimato dá conforto e poder, pois garante um alcance das palavras que fisicamente não se consegue. E isto traz problemáticas para as FSS, isto porque, os atores de esta ameaça podem surgir a qualquer hora de qualquer lugar, tendo uma capacidade de alcance brutal**."**
E8	"Através de uma análise de sentimentos e de um sistemático acompanhamento da sua evolução quer seja no sentido ascendente ou descendente."	- "A monitorização e análise massiva de dados, principalmente provenientes das redes sociais, permitem elaborar grafos indicadores de determinadas tendências." Por exemplo, um incremento exponencial em sede rede sociais de sentimentos contra uma determinada fação politica, religiosa ou uma determinada individualidade deverá ser tida em consideração, pois será um indicador de ameaça para com esses e a qual se poderá revestir de ações isoladas ou grupais, criminais ou de simples distúrbio público. Nesse âmbito as FSS devem ter essa análise em consideração para a adoção de mediadas preventivas e reativas."

Fonte: Autor

Quadro 14 - Sinopse das respostas à questão de entrevista n.º 12

Nº	Resposta	Sinopse
E11	"(...) nem todas as unidades da GC possuem estas capacidades técnicas, tanto de software, como de analistas (...) o uso das redes sociais implica um esforço da atividade da GC" (...)"	- "(...) é impossível monitorizar as redes sociais de modo permanente. São então necessárias ferramentas de *software* que possam fazer essa monitorização, dando um aviso quando exista um sinal de alerta e/ou um desvio fora do padrão" - "(...) dentro da *Jefatura de Información*, existe uma subunidade que trata da parte da informática, que desenvolve ferramentas de recolha e tratamento de informação, consoante os pedidos específicos dos analistas. Por ser uma unidade central,
E12	"Cada *jefatura* tem um serviço de monitorização (...) Existe também uma divisão de acordo com áreas de atuação."	"No entanto, o serviço de informações, e de policia judiciária, são os serviços centrais que estão dotados que maiores capacidades técnicas, que em caso de pedido destes serviços específicos, podem pedir uma monitorização concreta sobre um fenómeno especifico. Existe também uma divisão de acordo com as áreas de atuação, na parte das informações prende-se essencialmente com razões de estado (Terrorismo, Familia real, ataques a infraestruturas criticas), tudo o resto é da policia judicial."
E13	"Cada província tem uma monitorização especifica no âmbito da *securidad ciudadana"*	"Na parte das informações, mesmo na parte provincial existe uma dependência central da *jefatura de información*. Já na parte de policia judicial estes factos não se põem, pois são independentes."

Fonte: Autor

Quadro 15 - Sinopse das respostas à questão de entrevista n.º 13

Nº	Resposta	Sinopse
E10	"Quem tem competência de investigação relativa ao cibercrime na GC é a *Jefatura de Policía Judicial"*	- "A jefatura de Policía Judicial está dividida na UTPJ, UCO e no serviço de criminalística." - "A UCO é responsável pela parte operativa, enquanto a UTPJ é responsável pela parte de análise de informação criminal, desenvolvimento de ferramentas de *software* e bases de dados, cooperação internacional, e produção de relatórios de informações policiais e criminais." - "O serviço de criminalística tem um grupo com equipamento próprio para fazer perícias técnicas a equipamento informático com vista à recolha de prova digital." - " A principal dificuldade na investigação deste tipo de criminalidade prende-se com a recolha de prova com vista à identificação dos seus autores."
E14	"(...) a UCO tem capacidade de investigação total em matéria de cibercrime e criminalidade informática/ tecnológica"	- "A UCO é a unidade responsável pela investigação, uma vez que é esta a unidade responsável pela parte operativa da investigação criminal. - **"**Na UCO existe uma subunidade especializada em crime tecnológico, que por sua vez tem um grupo exclusivamente dedicado ao cibercrime e outro as redes sociais, que trabalham em estreita colaboração." - "Esta unidade trabalha em estreita colaboração com estruturas judiciárias também especializadas neste tipo de criminalidade". - "Tal como em todos os outros crimes, a UCO como unidade central só aloca para si casos de extrema complexidade e gravidade, ou quando se extravasa a competência técnica e territorial das unidades de policia judiciária de cada comunidade autónoma. - "Lidamos muito mais com casos de criminalidade tecnológica do que cibercrime, o que acaba por ser normal, pois hoje em dia quase todo o tipo de criminalidade tem um meio tecnológico envolvido. Nas redes sociais, vemos ultimamente muitos casos de burla, ameaças e *bullyng."*

Fonte: Autor

Quadro 16 - Sinopse das respostas à questão de entrevista n.º 14

Nº	Resposta	Sinopse
E11	"(...) centra-se essencialmente na primeira fase do ciclo de produção de informações, ou seja, na recolha"	- "Na parte das redes sociais, centra-se essencialmente na primeira fase do ciclo de produção de informações, ou seja, na recolha. Este manancial de informação é recolhido e armazenado, sendo depois pesquisada segundo filtros para produzir relatórios de informações policiais." - "É impossível fazer um uso direto da informação recolhida, a não ser em casos específicos. É preciso depois relacionar com outras fontes de informação."
E12	"(...) o mais importante na SOCMINT é o escolher o canal de informação adequado (...) é necessário utilizar também outros métodos de recolha de informações (...)"	- "É impossível ter uma unidade em que toda esta monitorização esteja centrada para todos os contextos, porque é impossível ter uma monitorização de tudo. Ou seja, é preciso uma especificação numa área concreta" - "Através de ferramentas de análise semântica é possível fazer esta análise, com base em taxionomia e modelos comportamentais, sendo possível ajustar consoante o contexto de monitorização. De referir, que a recolha de informação destas ferramentas é enorme, pelo que, uma análise à posteriori é necessária. Existem alguns perigos nesta atividade. Um dos critérios essenciais é definir qual a taxionomia a utilizar e o potencial de difusão dos perfis (famosos)." - **"**É importante ter pessoas especialistas, como tradutores, sociólogos, pessoas que conhecem a "realidade terreste" de um evento concreto, ou de uma realidade"
E13	"Após a recolha, e perante o âmbito que se pretende investigar é tratada a informação recolhida, sendo dividida naquela que tem interesse ou não."	- "Na *jefatura de información* toda a informação que é recolhida é tratada como confidencial (grau de segurança), dado as atividades que investiga. No caso da policia judicial já não é assim." - **"**No caso concreto da Catalunha, foram utilizadas as redes sociais no âmbito do ativismo e *hacktivismo*. Foram também utilizados no âmbito da coordenação de manifestações, utilizando *twitter,* canais de *telegram, whattsapp*. Esta coordenação existia ao nível dos cyber-neighbourhoods e depois ao nível central. Como exemplo temos o corte das autoestradas, e rutura das assembleias de voto." - "Foi também utilizado no âmbito de fazer ativismo contra pessoas que nutriam um sentimento nacionalista. Publicação de fotos em grupos dessas pessoas para controlar a sua vida."

Fonte: Autor

Quadro 17 - Sinopse das respostas à questão de entrevista n.º 15

Nº	Resposta	Sinopse
E11	"Vantagem: É a principal fonte de recolha de informação" "Desvantagem: Volatilidade (...)"	- "Vantagens: - É a principal fonte de recolha de informação, apesar de muita dela ser de pouca utilidade. - As pessoas contam nas redes sociais muita informação que estariam inibidas de dar ás autoridades diretamente. - "Desvantagens - É a volatilidade. As Coisas mudam rápido, o que necessita de uma permanente monitorização, o que é uma tarefa muito árdua de fazer de forma continua.
E12	"Vantagem: Capacidade de perceber a realidade social (...) antecipação de atividades criminais" "Desvantagem: Especialização (...) dispêndio económico"	- "Vantagens: A antecipação de atividades criminais; Grande capacidade de perceber a realidade social, como não é possível em nenhuma outra plataforma. Através Da sua atividade na rede social, dá para identificar uma pessoa com efeitos judiciais." - "Desvantagens: Para ter um valor concreto, é necessário um grande numero de recursos humanos e muito especialização dos seus ativos. Requer uma constante atualização quer da capacidade técnica (hardware e software) quer dos recursos humanos, e isto requer um grande dispêndio económico."
E13	**"**Vantagem: Compreensão de fenómenos criminais latentes" "Desvantagem: exige	- "Vantagens: As tecnologias de informação e da comunicação são utilizadas massivamente para orquestrar, organizar e planear atividades criminosas. Aos conseguirmos recolher estes dados das redes sociais e relaciona-los com outras fontes, conseguimos prever e direcionar o policiamento preventivo (...) evitando o

	grande capacidade técnica (...) dispêndio económico"	despoletar de um fenómeno criminal latente" - "Desvantagens: Para se conseguir extrair significado da informação recolhida nas redes sociais (...) são precisos muitos especialistas de várias áreas, que variam consoante o contexto de pesquisa e análise (...) o que leva um enorme gasto em termos de tecnologia e recursos humanos".

Fonte: Autor

ANEXOS

ANEXO A - UTILIZAÇÃO DAS REDES SOCIAIS

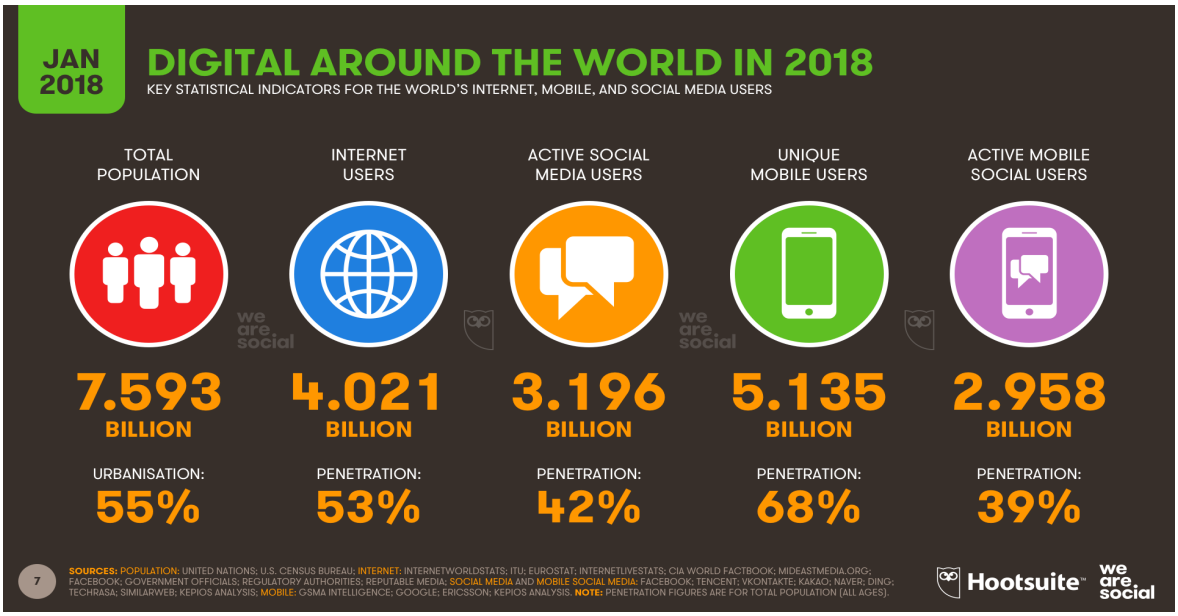


Figura 1 – Número de Utilizadores das Redes Sociais à Escala Global em 2018

Fonte: We are Social (2018)

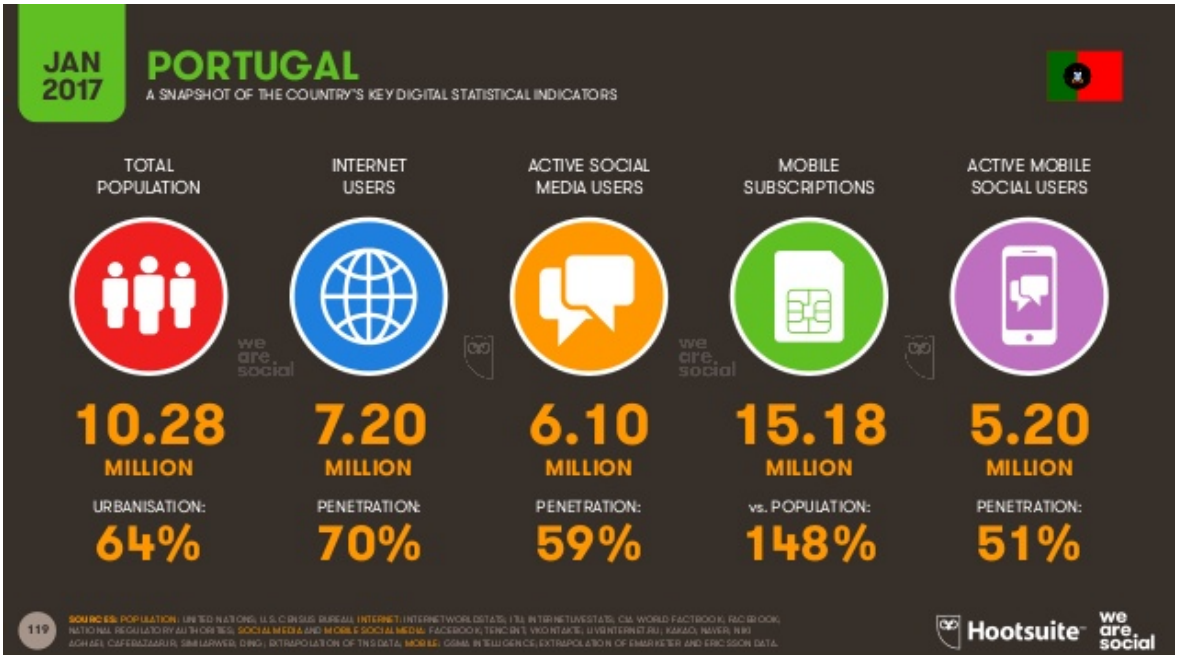


Figura 2 - Número de Utilizadores das Redes Sociais em Portugal no ano de 2018

Fonte: We are Social (2018)

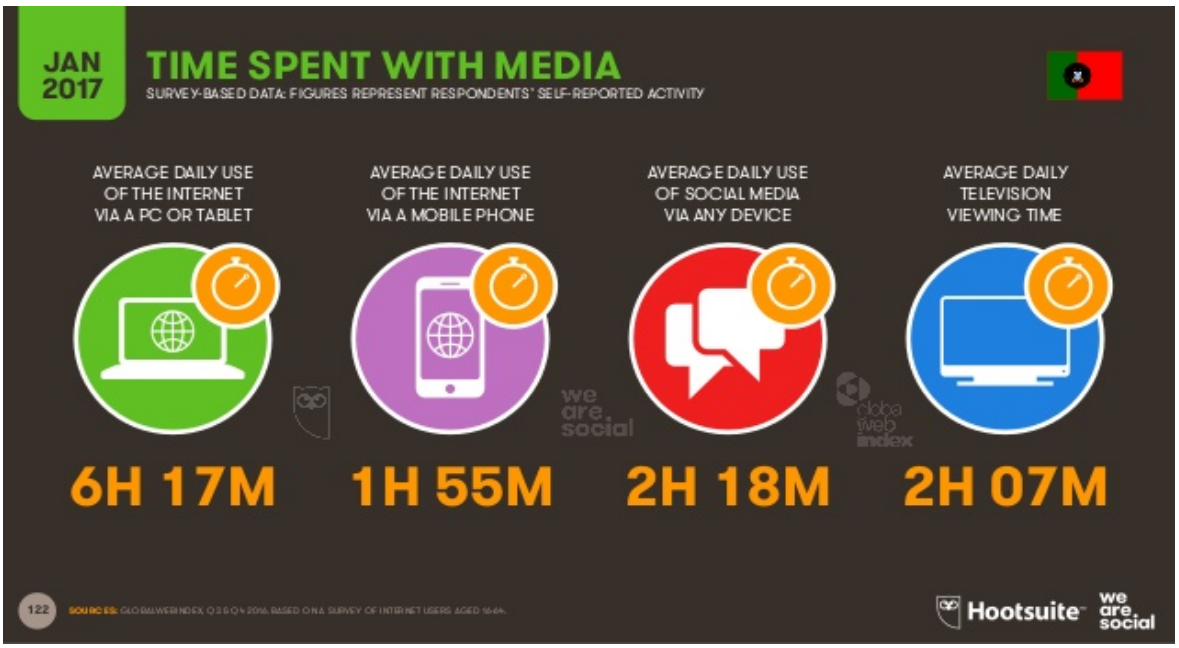


Figura 3 - Utilização Temporal das Redes Sociais

Fonte: We are Social (2018)

ANEXO B - ARQUITETURA CONCETUAL DA PLATAFORMA SENTINEL

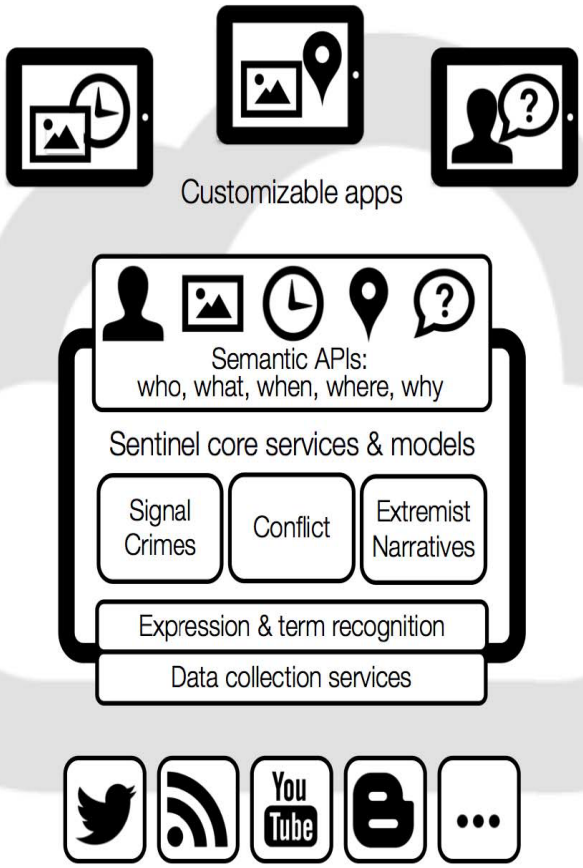


Figura 4 - Arquitetura Concetual da Plataforma Sentinal

Fonte: (Preece, et al., 2018)

ANEXO C - PIRÂMIDE DO DISCURSO DE ÓDIO

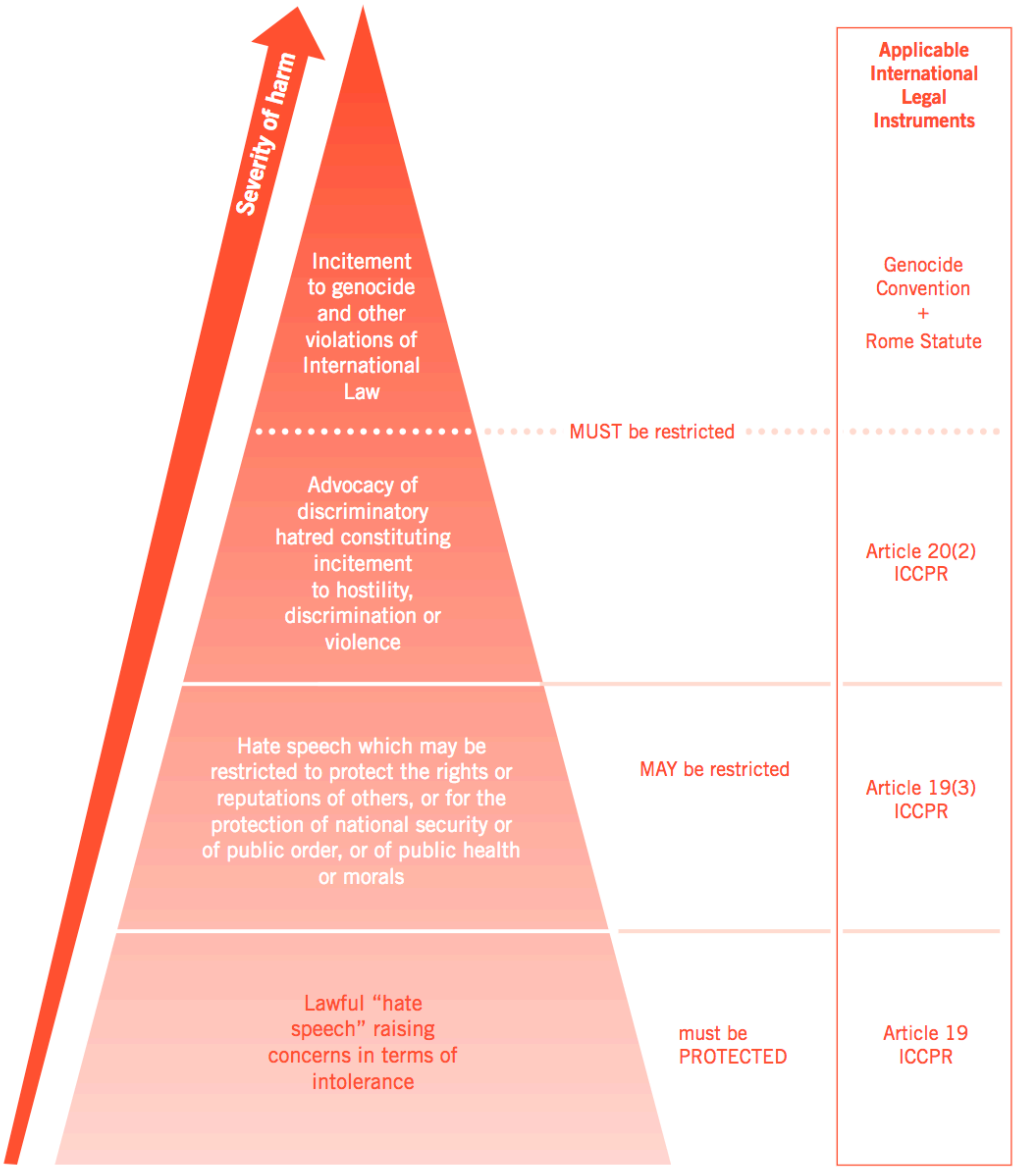


Figura 5 - Pirâmide do Discurso de Ódio

Fonte: (Article 19 [A19], 2015)