
**ACADEMIA MILITAR**

# A Investigação de Crimes Através de Meios Eletrónicos pela GNR

**Autor:** Aspirante de GNR Infantaria Diogo Alexandre Barreto Pereira

**Orientador: Major de Infantaria da GNR, Doutor, Tiago Silva**

**Mestrado Integrado de Ciências Militares na Especialidade de Segurança**

**Relatório Científico Final do Trabalho de Investigação Aplicada**

**Lisboa, 29 de maio de 2023**


**ACADEMIA MILITAR**

# A Investigação de Crimes Através de Meios Eletrónicos pela GNR

**Autor:** Aspirante de GNR Infantaria Diogo Alexandre Barreto Pereira

**Orientador: Major de Infantaria da GNR, Doutor, Tiago Silva**

**Mestrado Integrado de Ciências Militares na Especialidade de Segurança**

**Relatório Científico Final do Trabalho de Investigação Aplicada**

**Lisboa, 29 de maio de 2023**

# EPÍGRAFE

“Cheio de Deus não temo o que virá,

Pois venha o que vier, nunca será

Maior que a minha alma.”

*Fernando Pessoa, Mensagem, 1934*

# DEDICATÓRIA

À minha família.

# AGRADECIMENTOS

Ao meu orientador, o Sr. Major de Infantaria da GNR Tiago Silva, pelo apoio e contributo que sempre demonstrou estar disposto a dar, pela sua constante disponibilidade, independentemente do horário, ou dia da semana, e pela serenidade que sempre transmitiu, o que fez com que todas as críticas construtivas que foram feitas, elevassem a qualidade do produto final aqui demonstrado.

Ao diretor dos Cursos da GNR na Academia Militar, o Sr. Tenente-Coronel de Infantaria da GNR, Paulo Gomes, pela preocupação que demonstrou ao longo destes meses da elaboração do TIA.

Ao Sr. Tenente-Coronel Jorge Sanches e Silva, ao Sr. Major Joni Ferreira, chefe da SIIC do CTer de Vila Real, ao Sr. 1º Sargento Paulo Dias, chefe do NIC do CTer de Vila Real, ao Sr. 1º Sargento Artur Robalo, ao Sr. Cabo-Mor João Reis do NIC de Lamego, do CTer de Viseu, pela disponibilidade e celeridade com que responderam às entrevistas, sem as quais a realização deste trabalho não seria de todo possível, e por todo o conhecimento que me transmitiram, mostrando-se sempre prontos a auxiliar-me na elaboração deste estudo.

À minha família, nomeadamente aos meus pais, avós e madrinha, por todo o apoio, compreensão e ajuda que me deram ao longo desta longa caminhada que foi a Academia Militar, sem vocês não era possível.

Aos meus amigos, que de uma forma ou de outra contribuíram para me ajudar a ultrapassar algumas adversidades que foram aparecendo ao longo do caminho.

À Bárbara, por ter sido um dos meus pilares nesta jornada.

E por último, mas não menos importante, aos meus camaradas de curso, por tudo o que passámos juntos, todas as alegrias, todos os momentos menos bons, pela amizade que levo de cada um de vocês, e um agradecimento especial aos membros da Liga e àqueles que por motivos de força maior não podem possuir esse título, embora noutras circunstâncias seriam acolhidos de braços abertos.

A todos vós, o meu sincero bem hajam.

# RESUMO

O presente trabalho de investigação aplicada está subordinado ao tema "A investigação crimes através de meios eletrónicos pela GNR", e tem como objetivo principal, perceber de que forma a instituição procede à investigação de burlas através de plataformas digitais como sites de compra e venda de produtos, burlas com recurso a telemóveis ou computadores, e ainda através de plataformas eletrónicas de pagamento com o MB Way, dado o aumento que se tem vindo a verificar deste tipo de ilícitos criminais.

A investigação foi dividida em duas partes, uma teórica e uma prática. Na parte teórica procurou desenvolver-se um enquadramento teórico, onde se mostram os diferentes tipo de crimes relacionados com uso de meios eletrónicos e informáticos existentes, bem como, através de uma análise da legislação vigente em Portugal, perceber qual a competência da Guarda Nacional Republicana na investigação deste tipo de crimes. Na parte prática, aplicou-se uma estratégia qualitativa, tendo por base o método indutivo. Ao nível da recolha de dados e análise documental, esta foi feita através da realização de inquéritos por entrevista a militares da estrutura de Investigação Criminal da GNR.

Ao longo da investigação, foi possível perceber que ao longo da última década, os crimes realizados com recurso às novas tecnologias tem vindo a aumentar drasticamente, o que exige não só da GNR, mas também de todas as Forças e Serviços de Segurança, uma constante adaptação para poderem acompanhar a evolução da criminalidade.

Em suma, foi verificado que no seio da GNR existe já algum trabalho a ser realizado no que toca à investigação deste tipo de ilícitos, porém existirem várias lacunas que, sendo colmatadas, podem tornar a resposta institucional naquilo que os cidadãos esperam de uma instituição "próxima, humana e de confiança". Assim, a especialização dos militares nesta área, a aquisição de equipamentos capazes de fazer face às necessidades operacionais dos investigadores, são algumas das soluções que podem ser adotadas para atingir o objetivo da GNR, a segurança pública.



**Palavras-chave:** Burla; Plataformas digitais; Guarda Nacional Republicana; Investigação Criminal; Meios Eletrónicos.

# ABSTRACT

The present applied research work is focused on the theme "Investigating crimes through electronic means by the GNR" and has as its main objective to understand how the institution conducts investigations into fraud through digital platforms such as online buying and selling websites, fraud using mobile phones or computers, and also through electronic payment platforms like MB Way, given the increasing trend of these types of criminal offenses.

The research was divided into two parts, theoretical and practical. In the theoretical part, a theoretical framework was developed to showcase the different types of crimes related to the use of electronic and computer means, and through an analysis of the current legislation in Portugal, to understand the competence of the National Republican Guard (GNR) in investigating these types of crimes. In the practical part, a qualitative strategy was applied, based on the inductive method. Data collection and documentary analysis were conducted through interviews with members of the GNR's Criminal Investigation structure.

Throughout the investigation, it was possible to observe that in the last decade, crimes committed using new technologies have been increasing drastically, which requires not only the GNR but also all the Forces and Security Services to constantly adapt in order to keep up with the evolution of criminal activities.

In conclusion, it was found that the GNR is already conducting some work regarding the investigation of these types of offenses, but there are several gaps that, if filled, can make the institutional response align with what citizens expect from an institution that is "close, humane, and trustworthy". Therefore, the specialization of military personnel in this area and the acquisition of equipment capable of meeting the operational needs of investigators are some of the solutions that can be adopted to achieve the GNR's objective of public security.



**Keywords:** Fraud; Digital platforms; National Republican Guard; Criminal Investigation; Electronic means.

# ÍNDICE GERAL

# ÍNDICE DE QUADROS

# ÍNDICE DE FIGURAS

# LISTA DE APÊNDICES

# LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

**ATM-** *Automated Teller Machine*

**CP-** Código Penal

**CPP-** Código Processual Penal

**CTer-** Comando Territorial

**DIC-** Direção de Investigação Criminal

**DTer-** Destacamento Territorial

**FAP-** Força Aérea Portuguesa

**FSS-** Forças e Serviços de Segurança

**GNR-** Guarda Nacional Republicana

**IC-** Investigação Criminal

**LCI-** Lei da Criminalidade Informática

**LOIC-** Leio Organização da Investigação Criminal

**LPDPI-** Lei da Proteção de Dados Pessoais face à Informática

**MP-** Ministério Público

**NDP-** Núcleo Digital Forense

**NIC-** Núcleo de Investigação Criminal

**NTP-** Núcleo Técnico Pericial

**OPC-** Órgão de Polícia Criminal

**PJ-** Polícia Judiciária

**PTer-** Posto Territorial

**RASI-** Relatório Anual de Segurança Interna

**RCFTIA-** Relatório Científico Final do Trabalho de Investigação Aplicada

**TIA-** Trabalho de Investigação Aplicada

**TIC-** Tecnologias de Informação e Comunicação

# INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA) subordinado ao tema "A investigação de Crimes através de meios Eletrónicos pela GNR", surge no âmbito do Tirocínio para Oficiais da Guarda Nacional Republicana, sendo este um dos elementos base para o aproveitamento do curso.

Este trabalho visa a aplicação das competências adquiridas, bem como desenvolver a capacidade de compreensão dos domínios da segurança, tendo por base o estudo de um assunto que representa uma das áreas de trabalho da Guarda Nacional Republicana, neste caso a investigação de burlas com recurso a plataformas eletrónicas e digitais, e avaliar os desafios e o impacto que estes trazem para a atividade operacional da instituição, ameaças estas que são cada vez mais recorrentes devido ao crescente número de ciberameaças e, nomeadamente da cibercriminalidade.

Integrado na estrutura curricular do Curso de Formação de Oficiais da GNR, com destino à obtenção do grau de Mestre em Ciências Militares na especialidade de Segurança da GNR, surge, deste modo, o presente Trabalho de Investigação Aplicada, representando o culminar de cinco anos de formação, e apresentando-se como uma oportunidade para reforçar e aprofundar os conhecimentos que ao longo deste período foram transmitidos e adquiridos.

Com a realização deste trabalho pretende-se que se consolidem os conhecimentos de investigação no âmbito das Ciências Sociais, bem como que se coloque em prática a metodologia associada a uma investigação desta natureza, com o objetivo último de dar um contributo para a instituição quer a nível operacional quer a nível da sua imagem institucional, contribuindo desta forma para uma Guarda cada vez mais próxima, humana e de confiança.

Com a crescente utilização e o enorme alcance e magnitude das Tecnologias da Informação e Comunicação (TIC) em todas as esferas da sociedade, nomeadamente na Segurança e Defesa Nacional, a questão da Cibersegurança, devido à sua imprevisibilidade e natureza disruptiva, assumiu uma dimensão ao nível estratégico em todas as organizações.

A sociedade atual é extremamente influenciada pela *Internet*, mais concretamente pelo ciberespaço. No quotidiano, as interações sociais, os direitos dos cidadãos e também as economias estão dependentes, cada vez mais, do bom funcionamento das TIC.

O aumento da utilização dos recursos informáticos permite que haja uma recolha e partilha da informação em grande escala por parte da comunidade global. A *Internet*, como rede global de comunicação entre pessoas, assume um papel preponderante no processo de conexão e interligação dos mesmos.

A evolução e desenvolvimento da tecnologia transformou, portanto, o mundo numa sociedade global, na Era da Informação, o que proporcionou não só oportunidades, mas também riscos e ameaças provenientes do ciberespaço e que carecem de uma preocupação acrescida por parte das Forças e Serviços de Segurança (FSS).

A dependência da sociedade do uso do ciberespaço é, nos dias de hoje, um fator bastante crítico no que toca à economia e segurança, quer em termos individuais, quer em termos coletivos, como é o caso das organizações, uma vez que grande parte da informação pode ser acedida de uma forma mais ou menos direta ou imediata, através da *Internet.* Atualmente podemos aceder não só a informações pessoais através das redes sociais, mas também a informações críticas como por exemplo contas bancárias, estas últimas podem ser acedidas pelos próprios titulares, mas também por pessoas ou programas que consigam ultrapassar as medidas de Cibersegurança e Ciberdefesa por eles implementadas, colocando em perigo todos aqueles que se encontram ligados através da mesma rede (Martins, 2012).

O ciberespaço é entendido como uma extensão virtual do mundo real, e como tal, a atribuição de competências e responsabilidades neste âmbito deverá obedecer aos princípios legais e fundamentos que caracterizam a Segurança e a Defesa do Estado. Deste modo, as FSS assumem um papel crucial no combate à cibercriminalidade (Aparício, 2017).

A prática de condutas ilícitas neste novo ambiente denominado de ciberespaço, apresentam não só um estímulo para as FSS, mas também desafios, uma vez que estas deverão não só manter-se a par do desenvolvimento tecnológico e desenvolver ferramentas que lhes permita uma melhor investigação deste tipo de ilícitos criminais, evitando ficar obsoletas face à evolução que se verifica em toda a sociedade, mas também devido ao crescente número de intrusões a sistemas de vários órgãos e instituições nacionais e internacionais, tendo desta forma de proteger os seus sistemas e informação, fazendo uso das novas politicas de Cibersegurança Nacionais e Internacionais (Aparício, 2017).

Desta forma, a cibercriminalidade é considerada como um problema relevante e justificável na sociedade moderna atual, sobretudo considerando o potencial disruptivo que pode estar associado a um crime através de meios eletrónicos (Nunes, 2012).

A nível pessoal, este tema representa, não só pela sua atualidade (que obriga a que exista uma constante procura de novas estratégias e respostas às atuais ameaças e riscos),

mas também pela importância que traz para a instituição, e consequentemente para o exercício da profissão, algo com um elevado cariz motivacional, articulado com a importância que o objeto de estudo representa para a Segurança Nacional e, como tal para uma instituição como é a Guarda Nacional Republicana, e no que são os seus valores, missão e objetivos.

Tendo em conta os objetivos do presente Trabalho de Investigação Aplicada, este divide-se em quatro fases fundamentais, sendo a primeira fase a Introdução, em que é feita a apresentação do tema e do objeto de estudo. Esta encontra-se dividida em cinco pontos, enquadramento da investigação, importância e justificação do tema, definição dos objetivos, uma nota metodológica, e por fim os traços gerais em que está estruturado o trabalho.

Na segunda parte, constituída por dois subcapítulos, o primeiro tem como principal objetivo, fazer um enquadramento teórico, abordando os principais conceitos que estarão em estudo no trabalho, conceitos como o de cibercrime, ciberespaço, *Internet*, entre outros. É ainda neste capítulo que se irá fazer um paralelismo entre os vários conceitos em estudo, e que forma estes se influenciam mutuamente e em função uns dos outros. Irá ainda ser estabelecida a distinção entre burlas informáticas e burlas através de meios informáticos, sendo esta última o principal objeto de estudo deste TIA.

No segundo subcapítulo irão ser abordadas as competências relativamente à investigação criminal que a GNR possui para fazer a investigação deste tipo de crimes. Iniciar-se-á por um enquadramento legal, no qual nos debruçaremos sobre os principais textos legais referentes a esta matéria, como por exemplo a Lei do Cibercrime[1] ou a Lei Orgânica da Investigação Criminal[2]. Após a análise destes documentos, iremos abordar as competências específicas da GNR no que concerne à investigação de crimes/burlas através de meios informáticos, e como se processam estas investigações, e ainda perceber se a GNR possui as capacidades para realizar este tipo de investigações.

A terceira parte deste trabalho será a definição das linhas metodológicas orientadoras, perante os objetivos estabelecidos.

Por último, na quarta parte do trabalho, serão apresentadas as conclusões e considerações finais, com o objetivo de dar resposta à pergunta de partida, bem como às perguntas derivadas propostas.

[1] Lei n. º109/2009, de 15 de setembro – "estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico" – artigo 1º Lei n. º109/2009

[2] Lei n. º49/2008, de 27 de agosto – que define a investigação criminal e atribui competências de investigação criminal às diferentes FSS nacionais

Apesar de poderem não apresentar um carácter inovador, as conclusões a que iremos chegar assumem-se como academicamente válidas e procuram dar um contributo para a evolução da instituição no que a este assunto diz respeito.

# PARTE I – REVISÃO DA LITERATURA
# CAPÍTULO 1 – CIBERCRIME

## 1.1- Conceito de Ciberespaço e de Cibercrime

No início da década de 80, começaram a surgir desenvolvimentos no âmbito das telecomunicações, criando-se um espaço no mercado virtual, com a finalidade de propagar o volume de vendas de ideias, bens e serviços a uma escala mundial (Akdeniz, 2000, p.3). Ou seja, um mundo de seres, ambientes, atividades e códigos inteiramente renovados, eclodindo desta forma o conceito de "*Ciberespaço*", que engloba as comunidades intangíveis e o espaço interativo, sendo possível através do conjunto de redes que formam a *Internet* (Santos, 2015).

De acordo com a maioria dos autores estudados, o conceito de ciberespaço[3] surge no ano de 1982, através de uma crónica escrita por William Gibson, intitulada de "*Burnning Chrome"*, esta que, mais tarde, deu origem ao romance de 1984, "*Neuromancer*"[4] ("Neuromante", em português), do mesmo autor. Neste último, William Gibson refere-se ao ciberespaço como uma "representação gráfica do conjunto de dados computacionais existentes, retirados do sistema humano".

Apesar de ficção, o ciberespaço abordado por Gibson na sua obra, desenvolveu-se ao longo do tempo, chegando aos dias que correm como uma vasta dimensão de uso diário e massivo.

O ciberespaço pode ser descrito como um espaço relacional de troca imaterial, onde os indivíduos são capazes de interagir sem que haja necessidade de haver presença física, utilizando terminais de redes para a troca de dados interpessoais (Saavedra, 1998, p. 322).

O termo ciberespaço pode ser definido como um domínio que se caracteriza pelo uso de equipamentos eletrónicos e do espectro eletromagnético para armazenar, modificar e trocar dados por meio de sistemas de rede (Santos, 2016). Esse conceito é dinamizado por um conjunto de políticas associadas à Sociedade da Informação, proporcionando uma vasta gama de recursos e contribuições para organizações mundiais, infraestruturas e cidadania em geral (Freire, 2012, p. 53).

De maneira geral, o termo ciberespaço é frequentemente utilizado para se referir à

[3]"Ciber" deriva do termo grego *Keyrnan*, que significa navegar ou controlar o "espaço".
[4] "Neuromancer" é um livro de ficção científica que introduziu novos conceitos para a época, como a inteligência artificial avançada e um ciberespaço quase que "físico".

*Internet* e às práticas socioculturais a ela associadas. No entanto, devido à sua natureza intrincada e capacidade de executar uma variedade de tarefas, o ciberespaço num sentido mais estreito é suscetível de uma abordagem multidimensional e, por isso, pode ser tido como o objeto de estudo em diversas áreas, como a tecnologia, a estratégia, a segurança ou a política, para uma melhor compreensão do assunto (Santos, 2016).

O conceito de ciberespaço, que é muitas vezes confundido com o conceito da própria *Internet*, pode ser desmistificado, e entendido pelo "conjunto dos sistemas informáticos como o *hardware*[5], *software*[6], redes de comunicação, equipamentos e meios de comunicação e informação neles processados e armazenada" (Fernandes, 2013). Desta feita, pode considerar-se que o ciberespaço pode incorporar duas dimensões. Uma, representada pela componente não física, o espaço do ciberespaço, um lugar virtual no espaço virtual, ao qual podemos aceder e comunicar, o que contribui para a interação social do ser humano. Por outro lado, tem-se a componente física, ou seja, a perspetiva dos mecanismos ou estruturas eletrónicas, que permitem usar o ciberespaço (Barbosa, 2016).

As características e potencialidades do ciberespaço contribuíram para melhorar a qualidade de vida humana e apoiar o desenvolvimento da sociedade atual. Em sociedades altamente avançadas tecnologicamente, sistemas essenciais para atender às necessidades básicas dos cidadãos, como gestão e abastecimento de eletricidade, água potável e serviços financeiros, operam e dependem do ciberespaço. Isso ocorre porque esses sistemas, em grande parte pertencentes ao setor privado, são gerenciados por computadores ou sistemas em rede (Moreira, 2012).

O papel do ciberespaço na disseminação de informações tem sido crucial, como evidenciado em casos como a Primavera Árabe[7], em que a aspiração dos povos foi divulgada para a comunidade internacional por intermédio da informação transmitida pelo ciberespaço,

[5] *Hardware* - todo componente físico, interno ou externo dos computadores, ou telemóveis, que determina o que um dispositivo é capaz e como pode ser utilizado. Embora dependa de um *software* para funcionar (e vice-versa), o *hardware* é um elemento igualmente importante.

[6] *Software* - todo programa rodado em computadores, telemóveis ou outros dispositivos que permite a execução de suas funções.

[7] Foi uma onda revolucionária de manifestações e protestos que ocorreram no Médio Oriente e no Norte de África, a partir de 18 de dezembro de 2010. Houve revoluções na Tunísia e no Egito, uma guerra civil na Líbia e na Síria; também ocorreram grandes protestos na Argélia, Bahrein, Djibuti, Iraque, Jordânia, Omã e Iémen e protestos menores no Kuwait, Líbano, Mauritânia, Marrocos, Arábia Saudita, Sudão e Saara Ocidental.

ou manifestações como a Geração à Rasca[8], ocorrida em Portugal em março de 2011, e que foi organizada e convocada através do ciberespaço (Moreira, 2012).

No entanto, a realidade virtual também tem sido explorada para atividades ilegais por parte de organizações, tanto criminosas quanto não-criminosas, com uma variedade de objetivos e motivações, incluindo razões religiosas ou até políticas.

A ação de realizar atividades ilegais através ou contra o ambiente virtual é comumente chamada de ciberataques (Moreira, 2012). O RFA 390-6 define tais atos como aqueles que têm o objetivo de prejudicar a funcionalidade dos sistemas, sem fornecer uma definição clara do que constitui um ciberataque (Força Aérea Portuguesa, 2011, p. 1-3).

É evidente que o ciberespaço apresenta diversas características que o tornam altamente vulnerável a riscos e ameaças por parte de seus usuários. Essas ameaças são múltiplas e, de acordo com a literatura, podem ser classificadas em cinco dimensões principais: cibercrime, hacktivismo, ciberespionagem, ciberterrorismo e ciberguerra (Barbosa, 2016).

De acordo com o Capitão da Força Aérea Portuguesa (FAP) Dias Moreira (2012), um ciberataque é um:

> "ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, redes de computadores, sistemas e equipamentos".

Assim, os ciberataques, podem ser entendidos como todos os atos que influenciam negativamente o correto funcionamento de empresas ou Estados, aproveitando para tal a sua forte dependência das TIC (Santos, 2011).

Posto isto, é necessário entender as cinco dimensões referidas anteriormente, com maior enfoque no cibercrime, uma vez que se assume como o objeto de estudo do presente trabalho de investigação.

Relativamente ao *Hacktivismo*, pode dizer-se que a definição de *hacker* emergiu em meados dos anos 50, no MIT[9], e destinava-se a caracterizar aqueles que, com engenho,

[8] Foi um conjunto de manifestações ocorridas em Portugal e noutros países – nestes últimos, por parte de portugueses – no dia 12 de março de 2011. Foi uma das maiores manifestações não vinculadas a partidos políticos desde a Revolução dos Cravos, em 1974.

[9] Instituto de Tecnologia de Massachusetts, nos Estados Unidos da América, é uma universidade de pesquisa privada, localizada em Cambridge.

encontravam uma solução não ortodoxa para um problema complexa, mas de certa forma elegante (Santos, 2011).

A expressão *hacker* era referente a especialistas ou programadores que, procurando desenvolver o ciberespaço, indagavam por falhas nos sistemas, com o intuito de as colmatar, ou encontrar algo que pudesse ser criado de raiz (Militão, 2014).

Porém, muito por culpa do aparecimento do cibercrime, a este termo está associada uma conotação negativa, sendo os media os principais dinamizadores desta alteração, começando a usá-lo para retratarem indivíduos que cometem atos ilícitos com recurso a meios informáticos (Santos, 2011).

Na atualidade, *hacker* destina-se a impor um rótulo de cariz criminoso, que pode ir desde a pirataria, ao desenvolvimento e ativação de *malware*[10], (Militão, 2014), sendo agora considerado que um *hacker* é todo o indivíduo capaz de penetrar, explorar ou contornar *firewalls*[11] por forma a atingir o fim que o motivou a fazê-lo (Santos, 2011).

O *Hacktivismo* resulta assim, da utilização de conhecimentos informáticos para obter vantagens sobre empresas ou Estados, utilizando para isso as vulnerabilidades dos seus sistemas de redes, penetrando através dos seus *websites.* Apesar de serem praticados de forma ilícita, estes ataques podem pretender atingir fins lícitos ou não criminais, dependendo da motivação dos seus agentes, como é o exemplo dos *Anonymous*[12] que, ainda que façam do *hacking* a sua forma de atuar, os objetivos que perseguem passam também pelo apoio aos Estados no combate ao terrorismo (Berton & Pawlak, 2015).

Passando para o ciberterrorismo, este é comummente retratado como "todos os ataques altamente prejudiciais a computadores, projetados por indivíduos que procuram gerar o terror e o medo para atingir objetivos políticos ou sociais" (Warren, 2008).

Este tipo de ameaça dá-se através de uma combinação entre a prática do terrorismo tradicional enquanto atividade de cariz político ou social (Barbosa, 2016), com o objetivo de

[10] *Malware* é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas informáticos. O *malware* hostil, intrusivo e intencionalmente maldoso tem como objetivo invadir, danificar ou incapacitar computadores, tablets, dispositivos móveis, sistemas informáticos e redes, assumindo, frequentemente, o controlo parcial das operações de um dispositivo.

[11] *Firewall* é uma solução de segurança baseada em *hardware* ou *software* (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou receção de dados podem ser executadas. Assume um papel de barreira de defesa, bloqueando todo o tipo de dados indesejados pelo utilizador.

[12] O conceito tem sido adotado por uma comunidade *online* descentralizada, atuando de forma anónima e coordenada, geralmente em torno de um objetivo livremente combinado entre si e voltado principalmente a favor dos direitos do povo perante seus governantes. A partir de 2008, a comunidade de *hackers* Anonymous ficou cada vez mais associado ao *hacktivismo* colaborativo e internacional, realizando protestos e outras ações, muitas vezes com o objetivo de promover a liberdade na *Internet* e a liberdade de expressão.

instaurar pânico e terror nas sociedades, potencializando as características das TIC para atingir esse fim, a uma escala mundial (Davis, 2006).

Em suma, ciberterrorismo pode ser definido como o:

> "uso das TIC para a realização de ameaças ou [para] a organização (incluindo a troca de informação, angariação de seguidores e financiamento) e execução de ataques com grande impacto nas redes sociais e sistemas informáticos e nas infraestruturas críticas, motivadas por ideologias políticas ou religiosas, fomentando o medo e o terror, com o intuito de despoletar determinadas ações políticas" (Santos, 2014).

Abordando agora o conceito de ciberespionagem, tem-se que esta é uma derivação da espionagem dita tradicional, em que os Estados procuram obter vantagens estratégicas em relação a estados terceiros, através da aquisição de conhecimentos e informações sobre estes (Militão, 2014).

Segundo Santos (2014), a ciberespionagem é caracterizada pelo acesso a informação sensível, na maior parte dos casos com intenção de ter acesso a informações sobre projetos em desenvolvimento ou segredos de negócio, explorando para este fim, as vulnerabilidades existentes nos *websites* das organizações alvo. A mesma autora refe ainda que as motivações para este tipo de ações são motivadas pelas vantagens competitivas entre Estados ou empresas, que produzam projetos relacionados com a mesma área, ou ainda usar a informação recolhida para obter lucros financeiros com a sua venda.

Desta forma, pode dizer-se que a ciberespionagem tem o seu foco na aquisição de informações pertencentes a Estados ou empresas, informações essas que posteriormente irão constituir um benefício financeiro com a sua venda, ou quando usadas em benefício próprio, irão constituir uma vantagem estratégica perante outro Estado ou empresa (Instituto da Defesa Nacional, 2013).

A próxima dimensão a abordar das ameaças provenientes do ciberespaço é a ciberguerra.

Esta pode ser facilmente definida como "uma luta ou conflito entre duas ou mais nações ou entre fações dentro de uma nação, onde o ciberespaço é o campo de batalha" (Instituto de Defesa Nacional, 2013). Ou seja, o campo de batalha encontra-se materializado por uma dimensão digital, e os ataques e defesas centram-se em todo o tipo de estruturas e redes de computadores (Militão, 2014).

Em suma, todo o tipo de ataque, intrusão ilícita em redes ou computadores, bem como atos de ciberespionagem levados a cabo por Estados ou Governos ou ainda por atores independentes, podem ser considerados atos de ciberguerra. Estes atos, por sua vez, estão

maioritariamente ligados a conflitos existentes no mundo real, como conflitos políticos ou militares (Martins, 2012).

A última dimensão das ameaças provenientes do ciberespaço, é então o cibercrime.

Aos dias de hoje, existe bastante divisão entre os autores à cerca do conceito de cibercrime. Porém, pode ser considerado como um crime tradicional em que é utilizada a informática para o perpetrar, ou seja, pode ser praticado no mundo físico, mas tem implicações diretas com o uso da tecnologia e nomeadamente da *Internet*, de acordo com Feliz Gouveia, no *Dicionário Crime, Justiça e Sociedade* (2016, p.78).

Este, assume-se como um tipo de crime em que seja usado um computador ou uma rede de computadores, ou dispositivos de *hardware*, desempenhando o papel de agente perpetrador do crime, ou sendo apenas um facilitador ou alvo do crime (Symantec Corporation, 2013).

Os cibercrimes, podem também, na senda do que foi referido anteriormente, ser entendidos como atos através dos quais são atingidos objetivos criminosos, em que o computador ou computadores, servem de meio para atingir esse fim, são apenas um alvo simbólico desse ato ou assumem-se como o objeto do crime em si (Marques & Martins, 2006). Há ainda autores que defendem que estes crimes podem ser divididos em duas categorias distintas, os crimes próprios ou puros, que consistem em cometer o crime por meio da informática e contra um sistema informático, e os crimes impróprios ou impuros, nos quais o crime pode ser diversificado (Rodrigues, 2009).

Devido ao facto de não haver um consenso entre autores quanto ao conceito de cibercrime, é possível fazer uma distinção dos mesmos, entre "criminalidade informática em sentido amplo e criminalidade informática em sentido estrito" (Nunes, 2021). Assim, cibercriminalidade no sentido amplo, é aquela que pode ser cometida através de qualquer meio informático (Simas, 2014). Porém, para Nunes (2021), o mesmo crime pode ser praticado por via de outros meios, uma vez que a informática/*internet*, assumem-se apenas como instrumentos para a prática destes cibercrimes. Já o conceito estrito, engloba o bem jurídico em causa, ou seja, os autores consideram que apesar do bem jurídico a proteger não ser necessariamente digital, o meio informático é uma parte fundamental do tipo legal (Silva, 2022), como é exemplo a burla informática, constante na Lei do Cibercrime.

Estes crimes podem ainda ser divididos em três categorias, de acordo com a Comissão Europeia, crimes tradicionais (como a fraude ou a falsificação) no primeiro grupo; o segundo grupo engloba publicações de conteúdos ilegais em meios de comunicação *online*; e no

terceiro e último grupo pedem ser encontrados todos os crimes eletrónicos propriamente ditos, como por exemplo, a pirataria ou os ataques a sistemas informáticos (Amador, 2018).

Contrariamente, a Convenção sobre o Cibercrime, no Conselho da Europa (2001), e citando Gouveia no *Dicionário Crime, Justiça e Sociedade* (2016, p.78), veio estabelecer não três, mas quarto grandes grupos para combater o cibercrime: "ofensas contra a integridade, a disponibilidade e a confidencialidade dos sistemas informáticos e dos seus dados; fraude e falsificação informática; produção, disseminação e posse de conteúdos ilegais; e violação de direitos de autor e de propriedade intelectual".

Em suma, pode dizer-se que o cibercrime é todo o tipo de crime em que, independentemente da sua tipificação a nível legal, são utilizados meios informáticos, para executar atos ilícitos através de plataformas digitais, com repercussões no mundo real.

### 1.2 - Evolução da Internet Vs. Crescimento do Cibercrime

Cronologicamente, a Internet surgiu no início da década de 1960 como um projeto da empresa Research and Development (RAND) Corporation, financiado pela Força Aérea Norte-Americana, com o propósito de desenvolver redes de comunicação militar capazes de resistir a ataques químicos e nucleares (Alesso e Smith, 2006). Este projeto tornou-se essencial para as autoridades americanas durante a Guerra Fria[13], já que era necessário existir uma rede de comunicações resistente e segura, capaz de manter a comunicação em caso de catástrofes provenientes de um possível ataque por parte da União das Repúblicas Socialistas Soviéticas (URSS).

Anos mais tarde, em setembro de 1969, o Departamento de Defesa dos Estados Unidos da América (EUA), através da sua agência de pesquisa, a *Advanced Projects Agency (ARPA),* lançou a ARPAnet, uma rede de computadores que deu início ao que se conhece atualmente por *Internet* (Castells, 2015).

O termo "*Internet*" surgiu décadas após o início do desenvolvimento da tecnologia militar, quando o mesmo começou a ser utilizado para fazer ligações entre universidades americanas e institutos de pesquisa em diferentes países (Simas, 2014).

No início da década de 1990, surgiu o desenvolvimento comercial desta nova tecnologia com a criação da "*World Wide Web*", que continha um vasto conjunto de

[13] Foi um período de tensão geopolítica entre a União Soviética e os Estados Unidos e os seus respetivos aliados, o Bloco Oriental e o Bloco Ocidental, após a Segunda Guerra Mundial. O termo "fria" é usado porque não houve combates em larga escala diretamente entre as duas superpotências, mas cada uma delas apoiou grandes conflitos regionais conhecidos como "Guerras por Procuração".

informações organizadas em formato de texto, imagens, arquivos de áudio e vídeo, acessíveis aos consumidores através de *links* (Simas, 2014).

Embora o objetivo original da criação da tecnologia tenha se tornado obsoleto, a *Internet* passou a ser acessível a toda a população mundial, tornando-se num espaço cibernético sem fronteiras e dando origem ao que é agora conhecido como Sociedade da Informação (Simas, 2014).

Dada a sua versatilidade, é correto afirmar que a *Internet* desempenha um papel crucial na sociedade atual, uma vez que serve de suporte a uma vasta gama de organizações governamentais, económicas, militares, de telecomunicações, educacionais, de transportes, entre outras. Esta dependência dos sistemas informáticos, levou a que o cibercrime ganhasse uma expressividade cada vez maior, tornando-o num fenómeno frequente, perigoso e violador de direitos fundamentais.

Pode desta forma afirmar-se que a evolução da *Internet* e o aumento do cibercrime estão profundamente conectados, e são diretamente proporcionais.

Conforme mencionado anteriormente, a segurança no ciberespaço evoluiu para uma nova realidade onde os perpetradores de crimes virtuais são capazes de se esconder atrás de rostos invisíveis, tornando-se cada vez mais difícil identificar a autoria de suas ações. Aqueles que violam a privacidade dos usuários e ultrapassam as barreiras físicas dos Estados são frequentemente rotulados como *hackers*. Porém, importa salientar que existem dois tipos diferentes de *hackers*, os *"hackers de chapéu branco"* e os *"hackers de chapéu preto"* (Martins, 2012).

Assim, os *hackers de chapéu preto* são indivíduos envolvidos em atividades criminosas no ciberespaço, explorando as vulnerabilidades dos sistemas para invadir e/ou roubar informações de indivíduos ou organizações (Silva & Silva, 2021).

Deste modo,

> "Um chapéu preto é quem viola os sistemas de segurança cibernética para obter acesso ilícito a um computador ou uma rede. Se um hacker chapéu preto descobre uma vulnerabilidade de segurança, ele fará a exploração sozinho ou alertará outros hackers sobre a oportunidade, normalmente em troca de dinheiro" (BELCIC, 2020).

Em suma, de acordo com Ivan (2020), "os hackers de chapéu preto" podem ser iniciantes na difusão de *malwar*e, bem como *hackers* altamente habilidosos e experientes que têm como objetivo roubar informações pessoais, credenciais de login e dados bancários.

Um *hacker de chapéu branco*, por outro lado, é um *hacker* que utiliza os seus conhecimentos em informática para tentar invadir um sistema, mas com o objetivo de

identificar as vulnerabilidades e relatá-las à organização responsável pelo sistema. Muitos destes *hackers* são contratados por empresas para manter suas redes ou sistemas seguros (Silva & Silva, 2021).

Assim,

> "*Hackers* chapéu branco são o oposto dos *hackers* de chapéu preto. Eles têm os mesmos talentos, mas em vez de usá-los para fins criminosos, eles aplicam esses talentos para ajudar as empresas a fortalecer suas defesas digitais. Um *hacker* chapéu branco tentará intencionalmente violar um sistema, com permissão do proprietário, para identificar pontos fracos a serem corrigidos. Esse tipo de trabalho também é conhecido como "*hacking* ético" (BELCIC, 2020).

Há ainda quem defenda que existe uma outra vertente de *hackers*, os *hackers de chapéu cinza*, atuando em alguns momentos como *"whithe hat",* mas também pode atuar como *"black hat"*, porém sem causar danos demasiado sérios às organizações (Silva & Silva, 2021).

> "[...]Eles não são exatamente o modelo de altruísmo, como os *hackers* chapéu branco, nem se dedicam a atos criminosos. Enquanto os *hackers* chapéus branco obtêm permissão antes de sondar as vulnerabilidades de um sistema, os chapéus cinzas pulam essa parte e vão direto ao *hacking"* (BELCIC, 2020).

Conforme mencionado anteriormente, é evidente que o avanço das novas tecnologias impulsionou os fenómenos criminais ocorridos no ciberespaço. Isto deve-se ao fato de que, por um lado, a própria tecnologia pode ser objeto de práticas ilegais, enquanto que, por outro lado, a tecnologia suscita e potencializa novas formas de criminalidade ou modifica as formas já existentes (Simas, 2014).

Para fazer face a este problema, é necessário que haja um nível de segurança, fiabilidade e eficiência no seio da *Internet*, impondo-se desta forma a criação de uma segurança informática.

### 1.3 - Burla Informática Vs. Burla Através de Meio Informático

Uma vez que o cibercrime abrange várias vertentes, incluindo a burla informática, para estudá-la é essencial compreender primeiro os fundamentos da burla em si.

Segundo José Alfredo (2013), a burla tem início quando um ator tem a intenção de enriquecer ilegitimamente, usando para seu próprio proveito ou para proveito de outrem, factos que levem a induzir em erro ou enganar um outro ator "fazendo-a praticar atos que causem a ela mesma (ou a terceiros) um prejuízo de cariz patrimonial".

Deste modo é possível dizer que a característica essencial do crime de burla é a de induzir alguém em erro, isto é, "implica a colaboração da vítima, resultando numa viciação da vontade de que foi objeto" (Azevedo, 2016).

O crime de burla encontra-se tipificado no artigo 217.º do Código Penal (CP) Português[14].

De acordo com Alfredo (2013), o crime de burla é considerado um crime contra o património, e o bem jurídico a ser protegido é o património do sujeito passivo globalmente considerado. Portanto, a burla não pode ser classificada como um crime contra a propriedade, uma vez que, de acordo com Azevedo (2016), os crimes contra o património exigem que o prejuízo patrimonial seja um elemento do crime.

Segundo Albuquerque (2010), a astúcia mencionada no artigo 217º do CP refere-se à habilidade do agente em manipular a vontade do sujeito passivo através de uma falsa representação da realidade, criando assim um erro ou engano sobre os fatos. Esta astúcia é vista como uma vantagem cognitiva do agente sobre o burlado, e é usada como meio para enganar ou persuadir o mesmo.

Conforme destacado por Azevedo (2016), o erro é definido como a falsa ou inexistente representação da realidade correta que funciona como vício do consentimento da vítima, enquanto o engano corresponde à mentira contada pelo agente perpetrador do crime. Além disso, a autora ressalta que o crime de burla é apenas consumado se houver prejuízo patrimonial decorrente da sua prática, resultando no empobrecimento da vítima ou de terceiros.

Os crimes de burla têm, portanto, como base, induzir alguém em erro, de modo a obter algo para proveito próprio, sendo que, este tipo de fenómeno tem vindo a adaptar-se à realidade em que são praticados, assentando em princípios desonestos baseados na ganância e no desejo de poder (Silva, 2022).

No ano de 1617, o autor chinês Zhang Yingyu, escreveu e publicou um livro à cerca de contos e fraudes financeiras intitulado "*A New Book for Foiling Swindles, Based on World Experience"*. Este livro compila vários relatos de crimes de burlas e fraudes, exemplificando

[14] **Artigo 217.º do CP**
**Burla**
1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro engano sobre factos que astuciosamente provocou, determinar outrem à prática de atos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com pena de multa.
2 - A tentativa é punível.
3 - O procedimento criminal depende de queixa.
4 - É correspondentemente aplicável o disposto nos artigos 206.º e 207.º.

este tipo de crimes, e onde no final de cada conto é feita uma abordagem crítica, elogiando a capacidade intelectual dos vigaristas, e censura a falta de capacidade de compreensão das vítimas, culpabilizando-as por terem sido enganadas. Numa outra perspetiva, noutros contos, o autor faz uma reflexão moral sobre as ações levadas a cabo pelos vigaristas, mostrando que estas tipificam atos ilícitos e que não devem ser praticados. Durante a dinastia *Ming*, época em que foi escrito este livro, a China encontrava-se num processo de comércio internacional de bens, e como tal havia um grande movimento económico, o que potenciou o aparecimento destes esquemas, de modo a maximizar os lucros. Assim, a primeira edição desta obra tem como principal objetivo alertar a população para a existência destes esquemas e ajudá-las a evitar ser um alvo das mesmas, contudo, na maioria dos casos, este livro foi usado como sendo uma ferramenta para o desenvolvimento de burlas e fraudes, contrariamente ao seu propósito inicial (Silva, 2022).

Durante o século XIX houve um crescimento abrupto deste tipo de esquemas, muito por causa da falta de aviso para os mesmos, contrariamente ao que se verifica nos dias de hoje, onde estes são extremamente publicitados. Prova disso é a pouca abrangência que os meios de comunicação social possuíam na altura, o que não permitia alertar a população para este fenómeno, permitindo situações bastantes caricatas como a venda da Ponte de Brooklyn em diversas ocasiões. Apesar de tudo isto, os meios de transporte, nomeadamente os ferroviários eram usados com relativa facilidade, permitindo que que estas burlas nunca fossem praticadas no mesmo sítio, mas sempre em grande número e em sítios não muito distantes umas das outras. Os indivíduos que faziam destas práticas modo de vida eram apenas descobertos em casos em que as suas vítimas testemunhavam contra eles, fazendo descrições dos indivíduos e expondo os seus métodos (Silva, 2022).

O século XX ficou marcado pelos famosos *"Ponzi Schemes"*[15], que receberam este nome devido a um dos seus autores, Charles Ponzi. Estas fraudes consistiam em fazer com que as vítimas utilizassem o seu dinheiro para investir em negócios, com o objetivo de ter um retorno financeiro elevado, o que acabava por nunca se verificar, materializando-se num esquema em cadeia em que o lucro era apenas obtido por uns, após estes levarem outras pessoas ao engano. Nos dias que correm, este tipo de fraudes são conhecidas como esquemas

[15] Um esquema Ponzi é uma forma de fraude que atrai investidores e paga lucros a investidores anteriores com fundos de investidores mais recentes. Escolhido em homenagem ao empresário italiano Charles Ponzi, o esquema leva as vítimas a acreditar que os lucros vêm de atividades comerciais legítimas (por exemplo, vendas de produtos ou investimentos bem-sucedidos) permanecendo inconscientes de que outros investidores são a fonte dos fundos. Um esquema Ponzi pode manter a ilusão de um negócio sustentável, desde que novos investidores contribuam com novos fundos e desde que a maioria dos investidores não exija o reembolso total e ainda acredite nos ativos inexistentes que supostamente possuem.

em pirâmide, nos quais quem se encontra no topo é quem realmente enriquece, usando para esse propósito o investimento de novos associados que se inserem nas camadas mais baixas da pirâmide.

Tendo em conta tudo isto, pode afirmar-se que este tipo de ilícitos tem vindo a evoluir, sendo que os esquemas utilizados pelos criminosos variam e adaptam-se à realidade social em que vivem, tornando estes crimes extremamente difíceis de investigar, uma vez que a sua publicitação e o constante aviso para a possibilidade de ocorrência dos mesmos é uma constante por parte das FSS em colaboração com os órgãos de comunicação social (OCS). Pode observar-se que, de acordo com os Relatório Anual de Segurança Interna (RASI) da última década, existe um crescimento de crimes como a burla informática, a falsidade informática ou ainda o acesso ilegítimo. Da análise destes relatórios pode ainda verificar-se quem em Portugal os crimes de burla se encontram entre os mais participados, o que significa que apesar de todo o trabalho que tem vindo a ser feito de modo a prevenir estes crimes, este não é suficiente.

Através da análise dos dados presentes nos RASI da última década, é evidente que desde o ano de 2010, o uso de plataformas eletrónicas para a efetivação de burlas começou a constituir uma ameaça à segurança nacional uma vez que este tipo de fenómenos são imateriais, ou seja, é algo que só pode ser observado depois de ser concretizado (Silva, 2022).

Dado este problema, surgiu, em 2011 o primeiro programa de prevenção para os vários tipos de burla, o "Apoio 65-Idosos em Segurança", sensibilizando os idosos para este tema, uma vez que estes são os que mais sofrem deste tipo de crimes.

No ano de 2012 pode verificar-se que os crimes de burla são os mais participados no Sistema de Queixa Eletrónico, fazendo com que, também no ano de 2012, surgisse um programa especial, o "Gerações de Mãos Dadas", que se mostra em tudo semelhante ao programa anterior, dando a conhecer aos idosos esta forma criminal, e consequentemente assumir um papel de advertência para estes atos.

Em 2013 poucas alterações surgiram, apresentando-se como um ano bastante idêntico ao anterior.

Porém, o ano de 2014 assumiu-se como um ano de mudança de paradigma, onde surgem os dados mais relevantes para o desenvolvimento deste trabalho de investigação, com a inclusão no relatório dos crimes de falsidade informática e acesso ilegítimo, assumindo um papel de referência nos estudos realizados nos RASI (Silva, 2022).

A partir deste ano, em todos os RASI posteriores pode constatar-se que os crimes abordados anteriormente eram parte integrante dos mesmos, e aos quis é dado especial

enfoque. Analisando os dados que constam no RASI, pode observar-se que o número de burlas informáticas e nas comunicações participadas, atingiu o seu pico em 2019, com um aumento de 66,7%, podendo este aumento ser explicado devido à pandemia do COVID-19, que potenciou a ocorrência deste tipo de crimes; os crimes tipificados como "outras burlas", em 2017 , atingiram o seu ponto máximo, verificando-se um aumento de 47,9%; por fim relativamente aos crimes de acesso ilegítimo e falsidade informática, o seu pico foi atingido também em 2019, registando aumentos de 56,2 e 57,3% respetivamente. Analisando ainda o número de arguidos, podemos constatar através dos dados do RASI que, foi em 2014 que os crimes de burla informática e nas comunicações tiveram maior número, com 372 arguidos constituídos; o crime de acesso ilegítimo, com 54 arguidos, registou o seu máximo em 2015; e em 2019, o crime de falsidade informático registou o seu máximo de arguidos em processos, com 29 arguidos, sendo que todos estes dados podem ser consultados nas figuras 1 e 2.


| | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|---|---|
| Burlas Informática e nas Comunicações | 30,4 | 30,4 | 7,9 | -3,5 | 20,1 | 66,7 | 21,7 | 7,7 |
| "Outras Burlas" | -3,8 | 15,2 | 8,5 | 47,9 | -7,5 | -4,7 | 22,2 | 12,6 |
| Acesso Ilegítimo | 17,8 | 34,5 | 1,5 | 21 | -16 | 56,2 | 23,87 | -17,3 |
| Falsidade Informática | 36,1 | 73,7 | 37,6 | 16 | 12,2 | 57,3 | 45,4 | 4 |

**Figura 1**- Variação da Criminalidade (2014-2021)

**Fonte:** Silva (2022)

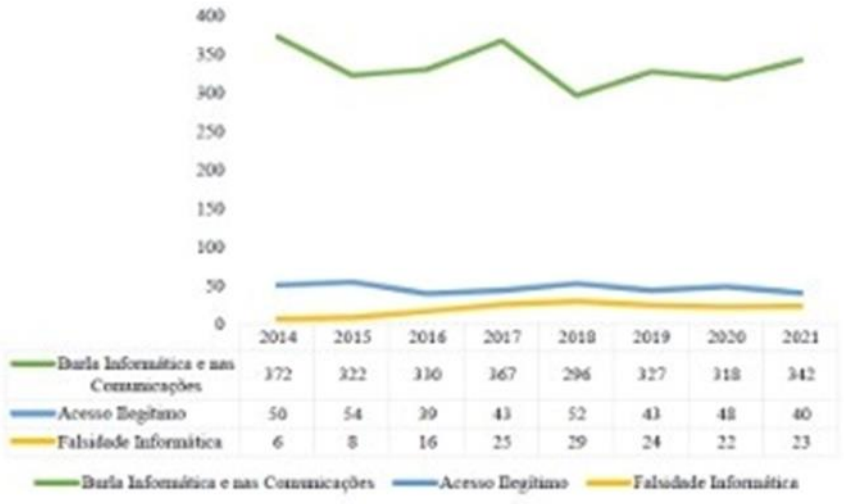


**Figura 2-** Variação do número de arguidos constituídos (2014-2021)

**Fonte:** Silva (2022)

Por outro lado, mas à semelhança da burla clássica, a burla informática partilha da mesma essência, ou seja, causar dano patrimonial a outra pessoa, utilizando para isso uma deturpação da realidade, e aproveitando-se desse facto para enganar a vítima.

No entanto, a diferença entre as duas consiste no facto de que a burla informática manipula os dados que estão a ser exibidos, para levar a vítima ao erro (Azevedo, 2016), ou seja, o erro ou engano da pessoa é causado diretamente sobre os dados ou aplicações informáticas.

Para Morgado e Vegar (2003), os crimes informáticos relacionam-se com "o acesso indevido a sistemas computadorizados, para obter informações, como no uso do computador e das redes virtuais para a obtenção de lucro ilegal".

Contrariamente do que acontece com a burla convencional, na burla informática não existe a intervenção de terceiros, ou seja, este tipo de burla não se destina a manipular a vontade de uma pessoa, nem tão pouco existe um "ato gerador do prejuízo patrimonial por alguém" (Santos, 2016), uma vez que no caso da burla informática o intermediário é o meio informático.

# CAPÍTULO 2 – INSTRUMENTOS LEGISLATIVOS

## 2.1. Ordem Jurídica Portuguesa

Apesar de sempre presente no ordenamento jurídico português, os casos de cibercriminalidade e o impacto que estes traziam à sociedade de então eram quase irrelevantes, ao contrário do que acontece atualmente, uma vez que o desenvolvimento das novas tecnologias tornou este tipo de crimes numa preocupação constante.

As leis portuguesas desempenham, desde cedo um papel bastante ativo na luta contra a Criminalidade Informática, tendo o legislador português recorrido, em grande parte, aos princípios diretos que constam no Relatório do Comité Europeu para os Problemas Criminais, do Conselho da Europa, editando a Lei n.º 109/91, de 17 de Agosto, seguindo a Recomendação n.º (89) 9 do Comité de Ministros aos Estados Membros, recomendação essa relativa à Criminalidade usando o computador (Marques & Martins, 2000, p.510).

Através da análise do CP de 1982, pode constatar-se que relativamente a esta matéria, imperava a proteção dos dados pessoais, retirado na Convenção Europeia para a Proteção das Pessoas no que toca ao Tratamento Automatizado de Dados de Carácter Pessoal (Santos, 2015).

A denominada Lei da Proteção de Dados Pessoais face à Informática (LPDPI), Lei n. º10/91, de 29 de abril, veio a ser alterada pela Lei n. º28/94, de 29 de agosto, e possuía um esquema geral de infrações, constantes do capítulo VIII, mais concretamente nos artigos 34.º a 43.º, muito mais vasto do que as então tipificadas no artigo 181.º do CP de 1982[16].

Em 1991, a Lei da Criminalidade Informática (LCI) foi publicada através da Lei n.º 109/91, de 17 de agosto, seguindo a Recomendação n.º 89/9 do Conselho da Europa. Nessa lei, estavam presentes definições para novos tipos de crimes que deveriam ser regulados, conforme recomendado pelo Conselho da Europa, e que foram sentidos no ordenamento jurídico nacional (Santos, 2015).

[16] O que tinha de interessante à data da sua publicação era saber se toda a previsão deste último preceito (artigo 181.º do Código Penal de 1982) estava ou não absorvida pelas disposições da nova Lei 10/91 de 29 de abril. Segundo Garcia Marques e Lourenço Martins a resposta parece ser afirmativa quanto ao n.º 1 desse artigo 181.º da versão anterior do Código Penal. Como referem "bastava confrontar o conteúdo das alíneas a) a d) do n.º 1 desse artigo 181.º com os artigos 34.º, números 1 e 3, artigo 37.º e 39.º da Lei da Proteção de Dados Pessoais face à Informática (LPDPI), para constatar que esta lei posterior regulava tudo o que estava previsto naquele preceito do Código Penal".
Acresce ainda que outras normas específicas estendiam as sanções ainda à obstrução ao acesso (tal como previa o artigo 35.º), à interconexão ilegal (artigo 36.º) e ao acesso indevido (artigo 38.º).

Presentes na LCI, faziam parte alguns crimes que constavam da "lista facultativa dos tipos criminais" da Recomendação 89/9, tais como a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima e a reprodução ilegítima de programas protegidos.

Em 2009, foi promulgada a Lei n.º 109/2009, também conhecida como a Lei do Cibercrime. Esta lei estabelece disposições penais e processuais, bem como disposições relativas à cooperação internacional em matéria penal, no âmbito do cibercrime e da recolha de provas através de suporte eletrónico. A Decisão Quadro n.º 2005/222/JAI, de 24 de fevereiro, que trata dos ataques contra sistemas de informação, foi transposta para o ordenamento jurídico interno, e a Lei do Cibercrime estabelece uma ponte entre o direito interno e a Convenção sobre o Cibercrime do Conselho da Europa, conhecida como Convenção de Budapeste (Venâncio, 2006).

A vertente processual da Lei do Cibercrime deve ser considerada com atenção especial do ponto de vista judicial e policial, uma vez que o seu alcance vai além da criminalidade informática. As disposições processuais da lei, de acordo com as alíneas b) e c) do artigo 11º, são cumulativas à investigação de muitos outros crimes. Portanto, aplicam-se a todos os crimes cometidos por meio de um sistema informático ou coisas em que a recolha de prova em suporte eletrónico é necessária, exceto em casos de interseções de comunicações e ações encobertas, conforme disposto nos artigos 18º e 19º da Lei do Cibercrime (Verdelho, 2010).

Segundo Fernandes (2013) a principal doutrina portuguesa distingue a criminalidade relacionada com a utilização de computadores e em especial a *Internet* em quatro grupos distintos:

Crimes que usam meios informáticos, sem alterar o tipo penal comum, correspondem a uma qualificação do mesmo crime. São exemplos o crime de devassa por meio da informática (art.º 193º do CP), o crime de burla informática e o crime de burla informática nas telecomunicações (art.º 221º do CP);

Os crimes relativos à proteção de dados pessoais ou da privacidade (Lei n.º 67/98, de 26 de outubro, transposta da Diretiva n.º 95/46/CE e a Lei 69/98, de 28 de outubro);

Os crimes informáticos no sentido estrito têm o bem ou meio informático como elemento característico do tipo de crime. Esses crimes são cometidos contra e por meio de computadores, onde este é o alvo da atividade criminosa. Isso inclui os crimes previstos na Lei do Cibercrime.

Considerando o que foi mencionado anteriormente, embora as normas processuais da Lei do Cibercrime estejam previstas num diploma próprio, elas também se aplicam a um amplo conjunto de processos que vão além do crime informático em si. (Dias, 2010).

## 2.2. Competência dos OPC de Acordo com a Lei do Cibercrime

Conforme estabelecido na alínea 1) do n.º 3 do artigo 7º da LOIC, cabe exclusivamente à Polícia Judiciária (PJ) a investigação dos crimes informáticos cometidos com o uso de tecnologia informática. Portanto, é crucial analisar a competência dos outros Órgãos de Polícia Criminal (OPC) para investigar os crimes previstos na Lei do Cibercrime (Fernandes, 2013).

Com base na competência dos OPC, é importante estudar com mais detalhe o regime estabelecido para a pesquisa e apreensão de dados informáticos, conforme previsto nos artigos 15º e 16º da Lei do Cibercrime.

No contexto do ciberespaço, as medidas processuais de pesquisa e apreensão de dados são equivalentes às formas tradicionais de busca e apreensão reguladas pelos artigos 174º e 178º do Código Penal (Verdelho, 2010).

A pesquisa de dados em sistemas informáticos mantém a sua natureza de busca, contudo, com algumas regras adicionais constantes no artigo 174º, n.º 1 do Código Processual Penal (CPP):

A busca informática é ordenada quando houver indícios de que dados relacionados a um crime ou que possam servir como prova, estejam armazenados num sistema informático (art.º 15º n.º 1 da Lei do Cibercrime);

A autoridade judiciária competente é responsável por ordenar a busca informática por meio de um despacho, e é aconselhável que esta, sempre que possível, presida à diligência, de acordo com o n.º 3 do art.º 174º do CPP (Mesquita, 2010).

Relativamente à apreensão de dados informáticos, os pressupostos funcionais da apreensão em processo penal, à semelhança da busca, também não se alteram (art.º 178º, n.ºs 1 e 3, do CPP), assim:

De acordo com Fernandes (2013), a apreensão abrange tanto os sistemas informáticos utilizados na prática do crime como os dados informáticos que envolveram ou estavam destinados a serem utilizados na prática do crime. Além disso, também são compreendidos quaisquer outros elementos que possam servir como prova, incluindo aqueles deixados pelo agente no local do crime (art.º 16º, n.º 1 da Lei do Cibercrime);

Estas apreensões de sistemas e dados informáticos são autorizadas, ordenadas ou validadas por despacho da autoridade jurídica, conforme explanado no n.º 3 do art.º 178º do CPP (Fernandes, 2013).

Tal como estabelecido no artigo 178º, n.º 4 do Código de Processo Penal, a Lei do Cibercrime também autoriza o OPC a efetuar apreensões sem autorização prévia da autoridade judiciária, durante uma pesquisa informática legalmente ordenada a um sistema informático, bem como em casos de urgência ou perigo na demora, conforme indicado no artigo 16º, n.º 2, da mesma lei. Nestas circunstâncias, as apreensões efetuadas estão sempre sujeitas a serem validadas pela autoridade judiciária, no prazo máximo de 72 horas, conforme o n.º 4 do mesmo artigo.

O Ministério Público (MP) é responsável pela direção do inquérito, sendo assistido pelos OPC, conforme estabelecido no artigo 263º, n.º 1 do CPP. Os OPC agem sob a orientação direta do MP e são funcionalmente dependentes deste, de acordo com o n.º 2 do mesmo artigo.

O art.º 2º da LOIC estabelece que a direção da investigação criminal é da responsabilidade da autoridade judiciária competente em cada fase do processo. O n.º 3 do mesmo artigo determina que os OPC devem comunicar ao MP o conhecimento de qualquer crime no mais curto espaço de tempo, sem ultrapassar os 10 dias, e sem prejuízo da adoção das medidas cautelares urgentes para assegurar os meios de prova, evidenciando assim a importância da colaboração entre os OPC e o MP (Dias, 2010).

Segundo Fernandes (2013), da conjugação de todos os pressupostos analisados até então, a GNR, enquanto OPC:

Possui competências para realizar a pesquisa e apreensão de dados informáticos, com o objetivo de garantir os meios de prova necessários no cumprimento de atos processuais que tenham sido devidamente ordenados pela autoridade judiciária competente;

Em colaboração com a autoridade judiciária competente, a GNR pode realizar a busca e apreensão de dados em crimes conexos que não sejam caracterizados como crimes informáticos, e que não envolvam diretamente o uso de computadores como objeto central do crime;

Caso tenha conhecimento de algum facto que constitui crime, incluindo no âmbito da Lei do Cibercrime ou em casos de competência reservada à Polícia Judiciária (PJ), e sem prejuízo dos casos previstos no art.º 8º da LOIC, a GNR deve realizar os atos cautelares necessários e urgentes para garantir os meios de prova e, no prazo máximo de 10 dias, enviar o processo para o OPC competente, comunicando à autoridade judiciária competente.

Considerando esses fatores, fica claro que a GNR deve ter conhecimentos, capacidades tecnológicas e recursos humanos adequados para realizar medidas cautelares envolvendo dados e sistemas informáticos, e que esses recursos devem ser integrados numa estrutura específica que permita que seus militares trabalhem nessa área.

# PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

# CAPÍTULO 3 - METODOLOGIA DE INVESTIGAÇÃO

Este capítulo contém todo o processo metodológico realizado no decorrer do trabalho, representando desta forma uma apresentação daquilo que Prodanov e Freitas (2013) definem como sendo o caminho a percorrer para a construção de conhecimento, e que não é mais do que os procedimentos adotados com vista a atingir o objetivo e que tem como finalidade responder às questões "quando? com quê? como? onde?" (Marconi & Lakatos, 2003).

Atualmente, a realidade académica das diversas instituições de ensino superior caracteriza-se, não só, mas também, pela realização de inúmeros trabalhos científicos, elaborados no âmbito das múltiplas unidades curriculares existentes, e que preenchem o programa curricular dos cursos de licenciatura, de mestrado e de doutoramento (Rosado, 2017).

Desta forma, no contexto da investigação científica, é imperativo que se faça referência às várias publicações científicas, que são disponibilizadas em quantidades, e com qualidade cada vez mais significativas, assumindo um papel de destaque na investigação.

Desta feita, a investigação científica deve caracterizar-se, segundo Rosado, por ser "sistemática, metódica, replicável, racional, empírica, objetiva, comunicável e cumulativa".

Pode ainda definir-se investigação científica como "o diagnóstico das necessidades de informação e seleção das variáveis relevantes sobre as quais se irão recolher, registar e analisar informações válidas e fiáveis" (Sarmento, 2008, p.3).

Assim, esta parte do trabalho socorre-se de vários subcapítulos, onde o objetivo é explicar o caminho tomado em toda a investigação, fundamentando os diversos caminhos tomados no decorrer da investigação com base na doutrina existente no âmbito do tema, e sempre com o fim a que nos propusemos em mente. Tendo isto em conta, é feita uma abordagem ao modelo de análise adotado ao longo da investigação, o método de abordagem e a estratégia da investigação, e ainda é demonstrado o caminho percorrido relativamente ao desenho da pesquisa. Ainda neste capítulo são abordadas as questões da amostragem e das técnicas de recolha e análise de dados.

## 3.1- Modelo de Análise e Objetivos de Investigação

De acordo com Quivy e Campenhoudt (2018), a construção de um modelo de análise é algo de elevada complexidade, uma vez que é a partir deste que se irá efetuar a

conceptualização do tema, juntamente com a problemática da investigação em causa. Estes são os pilares que se assumem como fundamentais para guiar aquilo que vai ser a observação e a análise (Quivy & Campenhoudt, 2018).

No seguimento do que foi dito anteriormente, Marconi e Lakatos (2003) consideram que para definir a condição final de uma investigação e o caminho a percorrer na busca de informação deve ser formulada uma Questão Central (QC), por forma a definir um problema de investigação, sendo que o objetivo principal do investigador é resolver este problema, dando resposta à QC, devendo medir-se o êxito deste processo pela avaliação da clareza, da pertinência e da precisão da resposta (Santos et al., 2019).

Assim, o presente estudo tem como QC, derivando esta do objetivo geral (OG), a seguinte:

"De que forma é conduzida uma investigação de crimes realizados através de meios eletrónicos, pela Guarda Nacional Republicana?".

Analisando esta questão, podemos afirmar que esta se encontra profundamente ligada não só ao OG, mas também se encontra na génese das questões derivadas (QD), que se assumem como a verdadeira intenção do investigador, e que advém dos objetivos específicos (OE) (Bryman, 2016).

Assim, formularam-se as seguintes QD:

QD 1: "Quais são os tipos de crimes realizados através de meios informáticos com maior expressão em Portugal?"

QD 2: "Quais são as estruturas dentro da GNR que fazem a investigação deste tipo de crimes? "

QD 3: "Quais os principais obstáculos colocados à investigação deste tipo de crimes?".

### 3.2- Estratégia de Investigação e Método de Abordagem

Depois de serem definidos os objetivos do trabalho, o passo seguinte é estabelecer uma estratégia de investigação que terá de ter em consideração o âmbito da problemática em estudo, sendo que de entre as opções de estratégias quantitativas, mistas ou qualitativas, o investigador terá de optar por uma delas (Vilelas, 2020).

Considerando que, relativamente a este estudo, existe uma relação indissociável entre o mundo real e a subjetividade do sujeito, que não é passível de ser traduzida em números (Santos et al., 2019), a estratégia qualitativa irá ser a estratégia a adotar na realização do mesmo.

Sendo o objetivo desta investigação verificar de que forma a GNR conduz investigações de crimes realizados através de meios eletrónicos, esta estratégia assume-se como a mais adequada à realidade que se pretende estudar, uma vez que o pretendido é obter um entendimento extenso e subjetivo sobre o tema, sem ter em conta a quantificação e pesquisa estatística.

Em seguida é necessário definir o método de abordagem, este que se encontra no mesmo patamar de importância da estratégia de investigação, uma vez que se trata da linha de pensamento que um investigador irá seguir durante o seu trabalho (Prodanov & Freitas, 2013). Na presente investigação irá ser utilizado o método indutivo, que se caracteriza por ser baseado em análise de dados e de resultados sobre um fenómeno particular, com o intuito de alcançar a generalização teórica. Assim temos que os dados que foram recolhidos nos Núcleos de Investigação Criminal (NIC) dos CTer de Vila Real, Viseu, e o contributo de militares ligados à estrutura de Investigação Criminal da GNR permitirão que seja feita uma generalização de procedimentos em toda a instituição.

### 3.3- Técnicas de Recolha de Dados

No que concerne às técnicas de recolha de dados, estas assumem uma especial importância, pois sustentarão todo o processo de recolha de informação e aquisição de resultados fiáveis, isto se, forem as mais adequadas à própria investigação (Sarmento, 2013).

Assim sendo, a recolha de dados foi efetuada em dois momentos distintos, sendo o primeiro respeitante à análise conceptual do problema, combinando as abordagens qualitativa, recorrendo a artigos científicos, livros e entrevistas já existentes, e quantitativa, utilizando dados constantes no RASI e da própria Guarda.

Nesta primeira fase, o trabalho desenvolveu-se maioritariamente através de plataformas virtuais, o que, de acordo com Saumure e Given (2008) é a forma que nos garante o maior acesso a informação, para além de que serve de enquadramento para a investigação, bem como para definir a problemática (Fortin, 2009).

Numa segunda fase, procurando complementar o trabalho até então desenvolvido, iniciou-se uma recolha de informação através de um método de observação não-participante, com recurso a inquéritos por entrevista, com o objetivo de obter "uma proporção de respostas suficiente para que a análise seja válida." (Quivy e Campenhoudt, 2018, p. 184), sendo que estas constituem ainda um elemento capaz de enriquecer o conhecimento na matéria por se tratar de elementos peritos ou especialistas na área de estudo (Sarmento, 2013).

De acordo com o pretendido quanto aos objetivos específicos, foram realizadas entrevistas semiestruturadas, com base num guião de entrevista (Apêndice B), previamente concretizado por forma a orientar a intervenção dos entrevistados (Silvestre, Fialho & Saragoça, 2014).

A todos os entrevistados foi aplicado o mesmo guião de entrevista, uma vez que todos eles desempenham funções na estrutura de IC da GNR, ou pelas funções que desempenharam num passado próximo na DIC assumem-se como especialistas no tema, dado o profundo conhecimento e experiência sobre a matéria em estudo.

Em todas as entrevistas, foi dado a conhecer aos entrevistados que estas seriam gravadas, bem como que qualquer parte que estes considerassem que devesse ser oculta do trabalho, o mesmo poderia ser feito.

### 3.4- Amostragem

Tendo em conta o universo que se encontra adstrito a esta temática, torna-se deveras incomportável estudar todos os elementos, pelo que foi necessário selecionar uma fração desse universo por forma a caracterizá-lo de forma eficaz (Marconi & Lakatos, 2003). Para obter uma amostra representativa a escolha desta fração não poderá ser feita fortuitamente (Jupp, 2006).

Desta forma, no seguimento do que foi dito anteriormente, foi aplicado um inquérito por entrevista a um grupo de militares que pertencem à estrutura de IC da Guarda Nacional Republicana, nomeadamente ao chefe da SIIC do CTer de Vila Real, ao chefe do Núcleo de Investigação Criminal (NIC) do DTer de Vila Real, e ainda a um militar que desempenha funções no NIC de Lamego, pertencente ao CTer de Viseu. Esta mesma entrevista foi ainda aplicada a dois militares com conhecimento suficiente na área da IC, tendo em conta as funções que desempenharam num passado próximo, na Direção de Investigação Criminal (DIC) da GNR, em complemento com a sua vasta experiência sobre o tema em estudo.

Assim, a amostragem caracteriza-se por possuir visões diferentes sobre o tema em estudo, abarcando tanto a parte da investigação criminal propriamente dita, como também os processos de recolha de informação e prova em meio digital, duas valências da Guarda Nacional Republicana que se encontram profundamente ligadas.

### 3.5- Análise de Dados

A recolha de dados, na estratégia qualitativa, é feita recorrendo a entrevistas, à observação e análise documental, sendo que neste Trabalho de Investigação Aplicada irão

ser realizadas entrevistas estruturadas, que consistem na abordagem de assuntos previamente determinados, de interesse para o trabalho, onde as perguntas são mais estruturadas e ordenadas (Sousa & Batista, 2011, pp. 80-81).

No que concerne à observação, esta será não participante, uma vez que o investigador será um ator externo que observa o fenómeno do lado de fora, sem se integrar na comunidade que está a estudar.

Por fim, a análise documental, que se constitui como uma técnica de investigação em que o trabalho se centra na recolha de fontes documentais onde se encontram registados princípios, objetivos e metas (Sousa & Batista, 2011, pp 88-89).

# CAPÍTULO 4 – APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

## 4.1- Apresentação, Análise e Discussão de Resultados dos Inquéritos por entrevista

Neste subcapítulo irão ser apresentados, analisados e discutidos os dados que foram obtidos através dos inquéritos por entrevista realizados durante esta investigação. Será ainda feita a comparação dos mesmos com o conteúdo analisado na pesquisa documental.

### 4.1.1- Apresentação, Análise e Discussão de Resultados da Questão Nº 1

A questão nº1 "Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?" tem como objetivo perceber quais os crimes associados ao uso de meios informáticos, eletrónicos ou através de plataformas digitais têm maior expressão na área de atuação da GNR.

A esta pergunta, de uma forma geral, todos os entrevistados referiram que a burlas online são os crimes que existem em maior número na área da GNR.

O E3 acrescenta ainda que estas ocorrem através de plataformas digitais, como o OLX, o WhatsApp ou o MB Way. O E4, para além das plataformas elencadas pelo E3, acrescenta ainda o Marketplace, e aborda crimes como o *phishing*, e crimes de extorsão, nomeadamente o *Sextortion.* Por sua vez, o E5 acrescenta a tudo o que foi referido pelos outros entrevistados, o crime de Cyberbullying, manifestando-se através de ameaças, difamações e extorsões.

### 4.1.2- Apresentação, Análise e Discussão de Resultados da Questão Nº 2

Relativamente à questão "Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?", tem como finalidade perceber de que forma a GNR procede no início da investigação deste tipo de crimes, e quais são os procedimentos que os militares devem ter em conta aquando do recebimento da notícia do crime.

Mais uma vez, as respostas de todos os entrevistados não apresentaram diferenças significativas entre si, como se pode constatar no quadro 3 do Apêndice H. Assim, todos referiram que para além dos procedimentos normais a tomar aquando do recebimento de

uma queixa de um crime desta tipologia, os militares da Guarda devem ter em atenção alguns procedimentos essenciais, tais como: obter uma descrição pormenorizadas sobre os factos; obter uma cópia ou uma impressão do anúncio, identificação da plataforma onde se efetivou a burla, com o respetivo ID do anúncio e referência URL do anúncio de venda colocado pela vítima; questionar a vítima sobre a data e hora da colocação do anúncio e a data e hora em que foi contactada pelo agente do crime. Tudo isto sobre a plataforma em que se preconizou o crime.

Relativamente ao suspeito, os militares devem procurar obter uma descrição sobre o interlocutor, nomeadamente características como o género, possível sotaque, erros ou especificidades na linguagem (se existirem), nome, localidade e outras informações que considerem relevantes, uma vez que, apesar da grande probabilidade de serem falsas, estas permitem detetar coincidências noutras narrativas idênticas, e associar o suspeito a ambas.

No que toca à vítima, os militares devem aconselhá-las a não apagar os dados e registos dos telemóveis, nomeadamente as mensagens SMS ou de correio eletrónico que tenham recebido ou enviado; de preferência, recolher imagem de todas as mensagens ou de todos os registos que ainda estejam disponíveis nos telefones ou outros dispositivos do queixoso, mormente: números de telefone utilizados pelo agente do crime para contactar o ofendido; número de telefone inserido em ATM no momento da instalação da aplicação MB WAY (por vezes mencionado como número de referência), indicando no caso de contacto telefónico se o mesmo é pertença da vítima ou do agente do crime; deve estar descrito o Código PIN (código de 6 dígitos) indicado pelo agente do crime, que foi utilizado pelo denunciante para adesão ao MB WAY; em caso de existirem contactos por outra via, nomeadamente por correio eletrónico, indicar o endereço de e-mail do suspeito; identificação da conta e do(s) cartão(ões) bancário(s) associado(s); identificação do ATM em caso de levantamento por parte do agente do crime (local e entidade): se o ofendido não tiver cancelado o cartão MB, retirar, de imediato, em ATM as informações disponíveis, nomeadamente sobre a entidade e o local de eventual levantamento (na caixa ATM selecionar "consultas" e depois selecionar "operações do cartão na rede Multibanco"); obter o extrato de movimentos do cartão – ver se a vítima sabe junto do banco a conta de destino em caso de transferências ou pagamentos; deve estar descrito a hora das operações (levantamento bancário/ transferências) e o local onde foi efetivado o movimento; diligenciar pela preservação das imagens do ATM (para além dos 30 dias a que obriga o n.º 2 do Art.º 13.º do DL n.º 34/2013, de 16 de maio). O período de preservação de imagens,

não se deve limitar, à hora referida das operações, mas deverá abranger um período mais alargado; se a vítima efetuou reclamação junto do banco, juntar cópia da mesma.

Existem ainda, neste campo, alguns procedimentos que devem ser tomados pelos investigadores do crime, diligências que devem ser pedidas junto do MP, quando as investigações ocorrem na GNR, como solicitar de imediato às Operadoras de Telecomunicações a identificação do titular do cartão SIM (número de telefone), bem como todos os equipamentos – IMEI, onde o cartão esteve ativo e restantes números e utilizadores/titulares associados aos números ativos nesse IMEI; no caso dos cartões pré-pagos, rogar a indicação do local de venda daquele lote de cartões, para que eventualmente seja possível apurar a existência de imagens captadas através dos sistemas de videovigilância ou alguma informação junto do vendedor; por último e ressalvando o que foi dito anteriormente, se ainda não tiver sido solicitado, diligenciar pela preservação das imagens do ATM (para além dos 30 dias a que obriga o n.º 2 do Art.º 13.º do DL n.º 34/2013, de 16 de maio). O período de preservação de imagens, não se deve limitar, à hora referida das operações, mas deverá abranger um período mais alargado.

### 4.1.3- Apresentação, Análise e Discussão de Resultados da Questão Nº 3

No que à questão "Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?" diz respeito, o principal objetivo desta é perceber de que forma os agentes do crime procedem no que toca a burlas através de meios eletrónicos como telemóveis e computadores, ou até mesmo plataformas digitais.

Nesta senda, temos que no geral, todos os entrevistados referem que o agente do crime escolhe as suas vítimas através de plataformas de compra e venda de produtos online, e após um contacto com as mesmas, desenvolvem um processo ardiloso para levá-las ao engano.

Os E2 e E4 referem que existem dois métodos para efetuar estas burlas, no primeiro, o agente do crime propõe à vítima o pagamento do valor do produto através de plataformas de pagamento eletrónico, como o MB Way, onde o criminoso seleciona a opção de "pedir dinheiro" em vez de "enviar dinheiro", aproveitando o desconhecimento do funcionamento da plataforma por parte da vítima, observando-se desta forma um "enriquecimento por meio de erro ou engano sobre facto que astuciosamente provocou", sendo este um dos pressupostos do crime de burla, constante do artigo 217º nº1 do CP. O segundo método utiliza também o desconhecimento da vítima sobre o funcionamento de plataformas de

pagamento eletrónico, nomeadamente o MB Way, onde os criminosos procuram que as vítimas sigam as suas instruções associando a sua conta bancária, ao contacto telefónico do burlão. Para isto, estes dão indicação à vítima para se deslocar a uma caixa multibanco e selecionar a opção "MB Way", introduzindo o seu cartão bancário e código pessoal; registam o número de telemóvel indicado pelo criminoso e de seguida introduzem o código de segurança indicado por este para efetivar a burla; a partir deste momento, o burlão passa a ter acesso aos recursos financeiros do titular daquela conta bancária, subtraindo todo o seu conteúdo sem que a vítima se aperceba. Este método representa outro dos pressupostos do crime de burla, previsto no artigo 217º do CP, o de "determinar outrem à prática de atos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial".

Ainda sobre o engano ou indução em erro, o E5 refere que o criminoso procura criar uma relação de confiança com a vítima fazendo uma proposta extremamente vantajosa à mesma.

É também importante realçar que todos os entrevistados referem a plataforma MB Way como a mais utilizada e mais comum neste tipo de burlas.

### 4.1.4- Apresentação, Análise e Discussão de Resultados da Questão Nº 4

Com a questão "Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?", pretendeu-se perceber se existe algum tipo de relação entre as vítimas e o fenómeno criminal em estudo, isto é, se as características das vítimas seriam semelhantes tendo em conta o crime de que foram visadas.

De facto, existe uma semelhança entre as vítimas deste tipo de ilícito criminal, nomeadamente a falta de conhecimento relativo a plataformas online de compra e venda de produtos, e de plataformas de pagamento eletrónico, como se pode constatar pelo que foi dito pelos entrevistados, através da análise do quadro 5 do apêndice H.

Ainda sobre esta questão, o E5 salienta que para além da literacia digital da vítima, existem outros fatores que podem estabelecer a ligação das vítimas a este tipo de crime, como por exemplo "apresentarem um perfil de vulnerabilidade, por força da sua idade avançada, pouca instrução académica, deficiência ou doença".

### 4.1.5- Apresentação, Análise e Discussão de Resultados da Questão Nº 5

A questão "Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?" tem como objetivo identificar as estruturas

da GNR através das quais se processa a investigação de crimes com recurso a meios eletrónicos.

Apesar de parecer uma resposta fácil, há que referir que, tal como apontou o E1, é necessário tipificar o crime antes de realizar qualquer investigação, isto porque, muitas vezes os crimes tendem a ser tipificados como crimes de acesso ilegítimo ou de falsidade informática, crimes esses que são da competência da PJ, logo a GNR não os pode investigar. Posto isto, o E1 acrescenta que os crimes que são tipificados como burlas através de meios eletrónicos e cuja investigação é delegada na GNR, a sua investigação envolve toda a estrutura de IC da instituição, que se encontra definida no Despacho N. º18/14-OG, de 11 de março, bem como em legislação regulamentar subsidiária.

Os E2, E3, E4 e E5 abordam a questão de uma forma mais direta, indicando que a investigação deste tipo de crimes é feita pelos militares que compõe os NIC dos CTer, com participação ativa das secções de Inquéritos dos PTer. Porém, no caso de ser necessário algum apoio de cariz mais técnico, por exemplo na área da prova digital, são acionados os Núcleos Digitais Forenses e os Núcleos Técnico Periciais, uma vez que são especializados na realização deste tipo de procedimentos.

### 4.1.6- Apresentação, Análise e Discussão de Resultados da Questão Nº 6

O objetivo da questão "Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?" é saber, de acordo com a experiência dos entrevistados na matéria em estudo, quais são os maiores obstáculos que os investigadores encontram aquando da realização da investigação.

Tendo isto em conta, o E1 refere que não é correto generalizar ou identificar dificuldades, uma vez que este tipo de crime, tal como todos os tipos criminais, possuem as suas particularidades.

Já os E2 e E5, referem que a maior dificuldade que é colocada às investigações se prende com a identificação e localização dos autores do crime. Isto deve-se ao facto de que na maioria dos casos, os investigadores não possuem equipamentos apropriados, e a Guarda carece de profissionais especializados para rastrear os factos, o que leva a que a autoria e a materialidade estejam ausentes, estas que são provas essenciais para a constituição de crime.

Na perspetiva do E3, a aquisição de notícia de crime assume-se como o maior obstáculo às investigações pois, em muitos casos existe a ausência de elementos essenciais e necessários para a realização de diligências subsequentes, que são cruciais para a identificação dos autores,

Já o E4, refere que a demora no envio de informações por parte de instituições bancárias, informáticas e tribunais condiciona as investigações, na medida em que estas instituições não se encontram preparadas para responder ao volume de solicitações existente, o que acaba por atrasar as investigações.

### 4.1.7- Apresentação, Análise e Discussão de Resultados da Questão Nº 7

Relativamente à questão "Questão nº7: Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?", esta destina-se a verificar qual o grau de qualificação dos militares da GNR no que toca à investigação deste tipo de crimes, uma vez que é uma área bastante específica da criminalidade atual, tendo em conta que as novas tecnologias são algo recente, e em constante mutação e evolução.

Assim, o E1 afirma que não só neste tipo de crimes, mas de uma forma genérica, a formação dos militares da Guarda mostra-se insuficiente para que "seja assegurada uma resposta institucional que o cidadão, a sociedade e Portugal esperam de uma instituição secular que procura ser mais humana, próxima e de confiança".

Os E2 e E4, consideram também que existe uma lacuna na formação dos militares que investigam este tipo de crimes.

O E3, reitera a falta de formação e afirma ainda que esta deveria ser contínua e com troca de experiências e partilha de conhecimentos entre os militares da GNR bem como de outros OPC.

Por último, o E5 afirma que a informática evolui diariamente, sendo que a formação dos guardas é mínima, para além do facto de que atualmente, os equipamentos carecem de licenças e *software* em número suficiente para determinadas pesquisas. Afirma ainda que a legislação em vigor não acompanha esta tipologia criminal.

### 4.1.8- Apresentação, Análise e Discussão de Resultados da Questão Nº 8

A questão "Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?" pretende identificar de que forma é feita a formação dos militares que investigam os crimes com recurso a equipamentos eletrónicos.

O E1 afirma que apesar de não existir ainda um curso específico sobre esta matéria, este já está a ser pensado e projetado quanto ao seu conteúdo desde 2021.

De acordo com E2, apesar de não existir formação específica, no decurso das investigações são difundidas instruções/orientações sobre a temática, por forma a facilitar o trabalho de investigação.

Na ótica de E3, este tipo de fenómeno criminal é relativamente recente, pelo que os investigadores possuem apenas formação para a IC no seu sentido amplo. Sendo este um tema bastante específico, afirma que "se justifica que haja um curso também ele específico, para este tipo de crimes, à semelhança do que acontece com os crimes de violência doméstica e tráfico de estupefacientes".

O E4 refere que a autoformação e a partilha de experiências entre os militares, vão permitindo mascarar a sua falta de formação nesta área.

Já E5 afirma que nos NIC "não tem havido formações nesta área recentemente", pelo que os investigadores se socorrem dos elementos do NTP, porém, estes apenas realizam pesquisas nos aparelhos/equipamentos apreendidos, não fazendo posteriormente a correlação entre os dados que extraem.

### 4.1.9- Apresentação, Análise e Discussão de Resultados da Questão Nº 9

No que diz respeito à questão "Questão nº9: Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?", esta tem como objetivo perceber se a GNR possui os equipamentos e ferramentas necessários para os militares realizarem as investigações nas melhores condições.

Desta forma, pode que, de acordo com os E1, E3 e E5, a GNR carece de meios, porém, a instituição não está indiferente a esta situação, como se pode ver através da resposta do E3, que refere que apesar da de os meios nunca serem suficientes no seio da Guarda, esta tem vindo a fazer um esforço no sentido de acompanhar a evolução criminal, como por exemplo a criação do NDF. Acrescenta ainda que o surgimento de novas tecnologias como a Inteligência Artificial não tardará a ser utilizada pelos burlões para praticar crimes de uma forma mais eficiente, o que se irá apresentar como um desafio para a GNR, na medida em que terá de reforçar os seus meios, não só tecnológicos como também humanos.

E1 afirma que o desenvolvimento de uma estrutura de IC para assegurar uma resposta cabal e capaz, exige da instituição uma especialização e gestão de recursos, quer humanos quer materiais, aliando a um investimento financeiro contínuo no acompanhamento das evoluções das tendências criminais.

Para E5, existe uma "falta gritante de meios" para realizar a investigação deste tipo de criminalidade, sejam eles militares especializados, ou meios informáticos de pesquisa. Refere ainda que, dada a complexidade que a investigação destes crimes apresenta, a GNR poderia trabalhar com alguns engenheiros informáticos, por forma a colmatar a falta de especialização dos militares.

Já E2 e E4 consideram que o nível de investigação de crimes informáticos que são permitidos à Guarda investigar, através da análise da LOIC, não exige meios muito avançados de *software*/meios informáticos.

### 4.1.10- Apresentação, Análise e Discussão de Resultados da Questão Nº 10

No final da entrevista, aplicou-se uma questão aberta, "Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?", por forma a dar aos entrevistados a oportunidade de expressarem a sua opinião quanto a assuntos que não tenham sido abrangidos durante a entrevista.

Desta forma, E1, referiu que seria aconselhável realizar uma leitura acerca de documentos internos como "Utilização Fraudulenta da Aplicação MB Way".

E2 referiu que não haveria nada a acrescentar, enquanto que E3 considera que deveria haver uma revisão da LOIC, uma vez que esta cria alguns constrangimentos da forma como está atualmente, nomeadamente no que diz respeito à atribuição de NUIPC (Número Único de Identificação de Processo Crime).

De acordo com E4, deveria existir uma desburocratização na fase de investigação, o que levaria a uma maior celeridade a nível processual, e E5 aborda questões em que a Guarda sente algumas dificuldades, nomeadamente na obtenção de interseções em tempo real às redes sociais, como Facebook, Instagram, etc. Refere ainda que apesar de se tratar de comunicações passadas, a colaboração deste tipo de empresas é difícil de obter, uma vez que se encontram sediadas em países terceiros, e a legislação nacional não tem força de lei para se conseguir tal desidrato, o que cria uma imagem de impunidade face a estes crimes.

# CONCLUSÕES E RECOMENDAÇÕES

O presente Relatório Científico Final do Trabalho de Investigação Aplicada abordou o tema da investigação de crimes através de meios eletrónicos, e os procedimentos adotados pela GNR para esse efeito, com objetivo de identificar possíveis lacunas recorrentes das investigações, para que estas possam vir a ser corrigidas.

Toda a investigação foi desenvolvida com base num pilar fundamental, a QC "…" que, após uma recolha e análise de dados recolhidos através de entrevistas realizadas a vários militares da Guarda, foi possível obter resultados que permitiram alcançar algumas conclusões relativamente a esta temática.

Assim sendo, aliando a análise dos resultados obtidos com a abordagem conceptual feita numa primeira fase da investigação, chegamos ao capítulo atual, que se destina a abordar as perguntas a que nos propusemos dar resposta no início da investigação, a QC, e as QD, perguntas essas que derivam do objetivo geral e específicos, respetivamente.

Posto isto, relativamente à QD1 "Quais são os tipos de crimes realizados através de meios eletrónicos com maior expressão em Portugal?", temos que, os crimes mais comuns de serem realizados através de meios eletrónicos no nosso país são os crimes de burla, em que o agente do crime aproveita o perfil de vulnerabilidade da vítima (como por exemplo a sua idade avançada, a pouca literacia digital, baixa instrução académica, deficiência ou doença), para induzir esta em erro, colocando-a numa situação de fragilidade e vulnerabilidade. Pode ainda dizer-se que este tipo de crimes está normalmente associado à compra e venda de produtos por meio de plataformas digitais, como é o caso do OLX, do Standvirtual, do Marketplace, entre outras, e ainda a aplicações como o MB Way, utilizado para fazer pagamentos de forma eletrónica e que, na maior parte dos casos, é o meio de efetivar a burla, através de um de dois métodos. O primeiro consiste em propor o pagamento através da aplicação, nesta fase, o burlão, seleciona a opção de "pedir dinheiro" em vez de "enviar dinheiro", aproveitando desta forma a falta de conhecimento do cidadão sobre o funcionamento da aplicação para lhe subtrair elevadas quantias. O segundo método, um pouco mais elaborado, assenta no princípio de que o burlão leva a vítima a seguir as suas indicações, fazendo com que esta se desloque ao multibanco e selecione a opção "MB Way", introduzindo o seu cartão bancário e código pessoal, associando o número de telemóvel do criminoso à sua conta. Desta forma, o burlão passa a ter acesso aos recursos financeiros daquela conta, sem que as vítimas se apercebam, e efetivando a burla momentos após a

conclusão deste processo. Daqui, pode retirar-se que existem dois denominadores comuns no que toca a este tipo de burla, a vítima (apresentando-se como alguém vulnerável), e a indução em erro por parte do agente do crime.

No que diz respeito à QD2 "Quais são estruturas dentro da GNR Que fazem a investigação deste tipo de crimes?", pode concluir-se que de acordo com a LOIC, se o crime for tipificado como acesso ilegítimo ou falsidade informática, por força do método utilizado pelo agente do crime, a competência de investigação é da PJ. Porém, no caso de ser considerado burla, a competência é do OPC territorialmente competente. Assim, quando a GNR tem competência de investigação, esta é feita através das secções de inquéritos dos PTer, dos NIC dos DTer, e ainda, no caso de ser necessário apoio técnico são ativados os elementos do NDF e NTP.

Relativamente à QD3 "Quais os principais obstáculos colocados à investigação deste tipo de crimes?", podemos dividi-la em três perspetivas distintas, a perspetiva operacional, a da formação dos militares e dos recursos disponíveis para realizar a investigação destes ilícitos. Ao nível operacional, pode dizer-se que todos os tipos criminais possuem as suas particularidades e, como tal, este não foge à regra. Os militares, no decurso das investigações deparam-se com problemas como demora no acesso a dados por parte de instituições bancárias, informáticas e dos tribunais, uma vez que o volume de solicitações é de tal forma elevado, que estes não possuem capacidade de resposta para fazer face aos pedidos de informação. A aquisição da notícia do crime é outro dos constrangimentos com o qual os militares se deparam, porque muitas vezes há ausência de elementos essenciais e necessários para a realização de diligências subsequentes, que são cruciais para a identificação dos autores. E ainda a localização do infrator uma vez que, na maioria dos casos, os investigadores não possuem os equipamentos apropriados ou não possuem especialização nesta área, de modo que não lhes é tão fácil rastrear os factos, ficando ausente a materialidade e a autoria do crime, que são provas essenciais para a constituição de crime.

Ao nível da formação dos militares, embora já esteja arquitetado e projetado do ponto de vista do seu conteúdo, um curso de especialização, desde 2021, os militares ainda não possuem qualquer tipo de formação específica. Este tipo de fenómeno criminal é algo recente, e os investigadores apenas possuem formação para a IC no geral, no entanto, dada a especificidade do tema e o crescente número de crimes desta natureza, justifica-se que, tal como acontece com a violência doméstica e o tráfico de estupefacientes, seja criado um curso específico para os investigadores, por forma a darem uma melhor resposta ás solicitações

que lhes chegam, e não mascarar a falta de formação com troca de experiências entre militares, e muitas vezes a autoformação.

Por fim, na perspetiva dos recursos existentes na Guarda para a realização deste tipo de investigações, pode dizer-se que existe uma falta gritante de meios informáticos de pesquisa. Sabe-se que os meios nunca são suficientes para aceder às necessidades dos cidadãos, e o desenvolvimento de uma estrutura de IC capaz de dar a resposta que se espera de uma instituição "próxima, humana e de confiança" requer uma especialização e gestão mais adequada dos seus recursos, para além de um investimento financeiro que acompanhe a evolução das tendências criminais.

Para além do que foi dito anteriormente, importa realçar que a informática evolui diariamente, e vive-se uma era onde a Inteligência Artificial é cada vez mais utilizada, como tal, o seu uso para a realização de crimes de burla vislumbra-se como uma realidade próxima, e assim sendo, a GNR deve procurar reforçar os seus meios, quer humanos quer tecnológicos, tal como procurou fazer aquando da criação do NDF, que em muitos casos presta apoio aos NIC no que toca à análise dos dados dos aparelhos apreendidos, no entanto não procedem à correlação dos mesmos, fazendo com que esta tenha de ser assegurada novamente pelos NIC.

Relativamente à QC "De que forma é conduzida uma investigação de crimes através de meios eletrónicos pela Guarda Nacional Republicana?", com a presente investigação foi possível observar que apesar da falta de meios e formação dos militares que fazem a investigação deste tipo de crimes, estes procuram manter-se atualizados, quer através da autoformação, quer através da troca de experiências e conhecimentos entre si, para que a resposta a este tipo de ilícitos seja dada o mais célere e competente possível. Dada a especificidade do tema, e a constante evolução das burlas, os investigadores desenvolvem um combate permanente a este tipo de crimes. No entanto, pode também observar-se que existem algumas lacunas quando se fala de investigação de crimes através de meios eletrónicos, muito por causa da falta de especialização dos militares, falta de meios e constante evolução do crime em si.

Assim tem-se que, para além dos procedimentos normais a adotar aquando da receção de uma queixa pelos militares, no processo de investigação, estes devem procurar saber certos aspetos do crime junto da vítima, nomeadamente a descrição pormenorizada dos factos, uma cópia ou impressão do anúncio, a identificação da plataforma onde se deu o

crime com o respetivo ID do anúncio e a sua referência URL; questionar a data e hora de colocação do anúncio e do contacto por parte do agente do crime; obter uma descrição do suspeito, abordando aspetos como o género, um possível sotaque ou especificidades linguísticas, o nome, a localidade, que muitas vezes apesar de falsos, permitem detetar similaridades com narrativas de outros crimes cometidos e reportados à GNR; os militares devem ainda procurar obter junto da vítima informações acerca da mesma, como imagem de todas as mensagens ou registos que tenham sido feitos através dos equipamentos eletrónicos; em caso de existirem contactos por outras vias, nomeadamente correio eletrónico, indicar qual o endereço eletrónico do suspeito; identificação da conta e cartão bancário associado; identificação do ATM, em caso de levantamento por parte do agente do crime; obter o extrato dos movimentos do cartão; e devem ainda alertar a vítima para não apagar qualquer dado ou registo do telemóvel, nomeadamente mensagens SMS ou correio eletrónico que tenham recebido ou enviado. Por último, os militares devem solicitar a identificação do titular do cartão SIM junto das Operadoras de Telecomunicações, bem como todos os equipamentos IMEI onde o cartão esteve inserido e titulares associados aos números ativos desse IMEI, para se conseguir uma possível identificação do suspeito.

Relativamente às lacunas identificadas na investigação deste tipo de crimes, temos, como já foi referido anteriormente, a falta de meios e conhecimento dos militares que fazem a investigação. Estes, possuem apenas a formação de IC no geral, não se encontrando capacitados com uma formação específica para este tipo de criminalidade, tendo estes que recorrer a estruturas como o NDF e o NTP, para fazer a extração dos dados dos equipamentos que são apreendidos, dados esses que posteriormente são devolvidos aos NIC para fazer a correlação dos mesmos. Muitas vezes, derivado do facto de os militares não estarem devidamente especializados para rastrear os factos, ficam ausentes a autoria e a materialidade, que são provas essenciais para a constituição de crime.

A nível de meios, no seio da GNR nota-se uma falta gritante de equipamentos técnicos na sua generalidade, e não só na investigação deste tipo de crimes, o que impossibilita os militares de darem uma resposta institucional adequada às necessidades do cidadão.

Relativamente às limitações deste trabalho, a principal é a limitação temporal para realizar o trabalho, o que leva a que a recolha de entrevistas para posterior análise de dados seja reduzida.

Para investigações futuras recomenda-se que seja feito um estudo comparativo com outros países com forças gendármicas que trabalhem este tema, e que seja feita um estudo da possibilidade e viabilidade de a Guarda se socorrer de engenheiros externos à instituição para colmatar a falta de formação dos militares.

# BIBLIOGRAFIA


Akdeniz, Yaman; Walker, Clive; Wall, David, *The Internet, Law and Society*, Longman, Pearson Education, 2000, p.3

Alesso, H. P. & Smith, C. F. (2008). *Thinking on the Web: Berners-Lee, Gödel e Turing*. Wiley-Interscience.

Amador, N. (2018). Cibercrime em Portugal. Trajetórias e perspetivas de futuro (1.ª ed.). Lisboa: Chiado Editora.

Aparício, M. (2017). *O ciberespaço como dimensão de segurança* (Doctoral dissertation).

Assembleia da República Portuguesa (2009), lei nº 109/2009 de 15 setembro - Lei do Cibercrime.

Assembleia da República Portuguesa (2018), Lei nº 46/2018 - Regime jurídico do Ciberespaço, DR nº 155 de 13/08/2018.

BARBOSA, M. L. As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal. Revista *de Direito e Segurança n. º8 (julho / dezembro 2016)*, 161-187.

Beattie, A. (2021, setembro). The Pioneers of Financial Fraud. Investopidia. Disponível em https://www.investopedia.com/articles/financial-theory/09/history-of-fraud.asp.

BELCIC, I. (2020). O que é hacking? Disponível em: <https://www.avast.com/pt-br/c-hacker>. Acesso em: 7 mar. 2023.

Berton, B., & Pawlak, P. (2015). *Cyber jihadists and their web*, (*January*), 1-4.

Bryman, A. (2016). Social Research Methods (5ª Edição). Oxford University Press

CASTELLS, M. (2015). A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar.

CM (2012), Resolução do Conselho de Ministros nº 42/2012, DR nº 74/2012, Cria a Comissão Instaladora do Centro Nacional de Cibersegurança (CNCS)

CM (2015), Resolução do Conselho de Ministros nº 36/2015, DR nº 113/2015, Estratégia Nacional de Segurança do Ciberespaço e atribuição de Autoridade Nacional ao Conselho Superior de Segurança do Ciberespaço (CNCS)

CM (2017), Resolução do Conselho de Ministros nº 115/2017, DR nº 163/2017, Cria o Conselho Superior de Segurança do Ciberespaço (CSSC)

CM (2019), Resolução do Conselho de Ministros nº 92/2019, DR nº 108/2019, Estratégia Nacional de Segurança do Ciberespaço (ENSC)

Creswell, J. (2013). Qualitative Inquiry & Research Design: Choosing Among Five Approaches. 3.ª ed. Los Angeles, CA: Sage.

Da Silva, A. L., & Da Silva, J. V. (2021). Ambientes seguros para trabalhar remotamente.

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

Decarli, G. C. (2018). História e evolução da internet. *Tendências do marketing digital*, 7.

Dias, V (2010). *A Problemática Da Investigação Do Cibercrime*, Universidade De Lisboa.

DPERI. (2014). Estratégia da Guarda 2020 - Uma Estratégia de Futuro. Lisboa: Guarda Nacional Republicana

Fernandes, F. (2013). *A cibersegurança e as estruturas críticas: A GNR: Ciberguarda, o futuro* (*Doctoral dissertation*, Academia Militar. Direção de Ensino).

Força Aérea Portuguesa, 2011. *Aprova a Política de Ciberdefesa da Força Aérea* (Regulamento da Força Aérea 390-6, de fevereiro de 2011), Alfragide, 2011.

Fortin, M., Côte, J. & Filion, F. (2009) Fundamentos e Etapas do Processo de Investigação. Lusodidacta

Instituto da Defesa Nacional. (2013). *Estratégia da informação e segurança no ciberespaço*. *Instituto da Defesa Nacional*.

IVAN, G. (2021). Cada hacker com o seu chapéu: o bom, o mau e o feio. Disponível em: <https://www.avira.com/pt-br/blog/hacker-e-chapeus-black-white-gray-hat>. Acesso em: 7 mar. 2023.

Jupp, V. (2006). The SAGE Dictionary of Social Research Methods. SAGE Publications. https://doi.org/10.4135/9780857020116

Maia, R. L., Nunes, L. M., Caridade, S., Sani, A. I., … Afonso, L. (2016). Dicionário Crime, Justiça e Sociedade (1.ª ed.). Lisboa: Edições Sílabo.

Marconi, M. & Lakatos, E. (2003). Fundamentos de Metodologia Científica (5ª Edição). Editora Atlas S.A.

Marques, G. & Martins, L. (2000) *Lições de Direito da Comunicação, Direito da Informática*. P.510. Almedina, Novembro.

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

Martins, M. (2012). Ciberespaço: uma Nova Realidade para a Segurança Internacional. *Nação E Defesa.*

Mesquita, Paulo (2010) *Processo Penal, Prova e Sistema Judiciário*

Militão, O. (2014). Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional. Dissertação de Mestrado da Faculdade de Ciências Sociais e Humanas, Faculdade Nova de Lisboa, Lisboa.

Monteiro, S. D., & PICKLER, M. E. V. (2007). O ciberespaço: o termo, a definição e o conceito. *DataGramaZero-Revista de Ciência da Informação*, *8*(3), 1-21.

Moreira, J. M. D. (2012). O Impacto Do Ciberespaço Como Nova Dimensão Nos Conflitos.

Morgado, M. J. e Vegar, J. (2003). O inimigo sem rosto: Fraude e Corrupção em Portugal. Lisboa: Publicações Dom Quixote.

Neto, Arnaldo Sobrinho de Morais, *Cibercrime e Cooperação Penal Internacional: um enfoque à luz da Convenção de Budapeste*, Universidade Federal de Paraíba – UFPB, João Pessoa, 2009, p. 41.

Nunes, D. R. (2021). Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime (2.ª ed.). Coimbra: Gestelegal.

Prodanov, C., & Freitas, E. (2013). Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. Universidade Feevale.

Quivy, R. & Campenhoudt, L. (2018). Manual de Investigação em Ciências Sociais. Gradiva

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

Rosado, D. P. (2017). *Elementos Essenciais de Sociologia Geral* (1ª). Gradiva

Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.322.

Santos, A. F. C. (2015). *O cibercrime: desafios e respostas do direito* (Master's thesis).

Santos, D. G. G. (2014). A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança.

Santos, J. L. A. dos. (2011). Contributos para uma melhor governação da cibersegurança em Portugal.

Santos, L.A.B., & Lima, J.M.M. (Coord.) (2019). Orientações metodológicas para a elaboração de trabalhos de investigação (2.ª ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sarmento, M. (2008). *Guia prático sobre a metodologia científica para a elaboração, escrita e apresentação de teses de doutoramento, dissertações de mestrado e trabalhos de investigação aplicada* (2.ª ed.). Lisboa: Universidade Lusíada Editora.

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

Saumure, K., & Lisa M.G. (2008). "Virtual Research." The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. http://www.sageereference.com/research/Article_n486.html

Silva, A. M. de S. e. (2022) *As competências e as capacidades da Guarda Nacional Republicana na prevenção e na investigação do crime de burla relacionada com o uso de plataformas eletrónicas de pagamentos.* Academia Militar.

Silva, J. J. (2019). *Apontamentos sobre cibersegurança e cibercrime.*

Silvestre, M., Fialho, I., & Saragoça, J. (2014). Word knowledge building Meta-evaluation of a Guide of Semi-structured interview. Da palavra à construção de conhecimento Meta-avaliação de um Guião de Entrevista semi-estruturada. Artículos de Ciencias Sociales, 3, 321–330.

Simas, DVD (2014). *O cibercrime* (dissertação de mestrado, Universidade Lusófona de Lisboa).

Sousa, M. J. & Baptista, C. S. (2011). Como fazer investigação, dissertações, teses e relatórios segundo Bolonha. 1.ª ed. Lisboa: Lidel.

Venâncio, P. (2006) – *Breve introdução da questão da Investigação e Meios de Prova na Criminalidade Informática*, Verbojuridico: Dezembro.

Verdelho, P (2010) "A nova Lei do Cibercrime", Lei nº 109/2009, Boletim da Ordem dos Advogados, nº 65

Vilelas, J. (2020). Investigação. O Processo de Construção do Conhecimento. Edições Sílabo

Warren, M. (2008). *Terrorism and the Internet*. *Cyber Warfare and Cyber Terrorism*, 129-153.

# APÊNDICES


# Apêndice A- Inquérito por Entrevista aos Militares da GNR

**ACADEMIA MILITAR**

**Cibersegurança: A Investigação de Crimes Através de Meios Informáticos pela GNR**

**Autor:** Aspirante de Infantaria da GNR Diogo Alexandre Barreto Pereira

**Orientador:** Major de Infantaria da GNR, Doutor Tiago Silva

**Mestrado Integrado de Ciências Militares na Especialidade de Segurança**
**Relatório Científico Final do Trabalho de Investigação Aplicada**
**Lisboa, abril de 2023**

## CARTA DE APRESENTAÇÃO

O presente estudo, com vista à elaboração do Relatório Científico Final do Trabalho de Investigação Aplicada, na Especialidade de Infantaria da Guarda Nacional Republicana, ministrado na Academia Militar, encontra-se subordinado ao tema "Cibersegurança: A Investigação de Crimes Através de Meios Informáticos pela GNR".

A necessidade de conduzir uma investigação sobre esta temática, deriva do facto de que a utilização das Tecnologias de Informação e Comunicação para a prática de ilícitos criminais, como as burlas, tem vindo a crescer ao longo da última década, tornando-se desta forma um problema para a segurança interna. Deste modo é objetivo desta investigação compreender de que forma a Guarda Nacional Republicana atua na prevenção e investigação deste tipo de crimes, bem como, perceber de que forma a formação dos militares da GNR os prepara ou não para fazer a investigação deste fenómeno criminal.

Portanto, com o propósito de obter informações relevantes e válidas relativamente às matérias supracitadas, solicito a Vossa Excelência que me conceda uma entrevista sobre o tema em apreço, tendo em conta que o seu contributo é fundamental para atingir os objetivos propostos para a presente investigação.

Grato desde já pela sua disponibilidade e atenção.

Atenciosamente,

Diogo Alexandre Barreto Pereira
Aspirante de Infantaria da Guarda Nacional Republicana

**PROTOCOLO DE CONSENTIMENTO INFORMADO**

O presente protocolo é estabelecido entre Diogo Alexandre Barreto Pereira, aluno da Academia Militar a realizar investigação com o tema "Cibersegurança: A Investigação de Crimes Através de Meios Informáticos pela GNR", e o participante_____ _ através do método de entrevista.

O investigador e o orientador científico comprometem-se a:

a) Conduzir a investigação de acordo com os parâmetros de qualidade preconizados pela comunidade científica da especialidade;
b) Discutir e negociar outros aspetos específicos de cada caso relativos à confidencialidade da informação, se solicitado pelo participante;
c) Impedir qualquer divulgação de informação referente aos participantes, exteriormente à equipa de investigação, sem o consentimento prévio de todos os envolvidos;
d) Entregar uma síntese descritiva dos resultados aos participantes, através de correio eletrónico;
e) Manter os participantes a par do trabalho que está a ser desenvolvido, nomeadamente no que concerne à análise dos dados, sempre que os mesmos o solicitem;
f) Prestar aos participantes no processo todos os esclarecimentos solicitados no decorrer da investigação;
g) Cumprir o Código Deontológico da *American Psychological Associantion* na realização da investigação;
h) Eliminar todas as gravações áudio após o decorrer da investigação e a defesa pública da tese.

Os participantes comprometem-se a:

a) Prestar informações sobre a sua experiência no caso em estudo e sobre a sua experiência profissional;
b) Ser entrevistado num momento acordado entre o investigador e o participante;
c) Autorizar a gravação áudio da entrevista, a pedido do investigador;
d) Decidir mencionar ou omitir a sua participação no projeto nos contextos profissionais em que considere conveniente fazê-lo;

e) Permitir a publicação do resultado do estudo, com omissão da sua identidade, nomeadamente nas seguintes situações:

I. Tese de Mestrado a apresentar à Academia Militar;

II. Comunicações em congressos científicos-profissionais;

III. Publicações científicas em revistas e/ou em livros da especialidade.

Assinaturas:

_____

(Participante)

_____

(Investigador)

Local e Data:

_____

**IDENTIFICAÇÃO DO ENTREVISTADO**

| | |
|---|---|
| **Nome:** | **Hora (Início/Fim):** |
| **U/E/O:** | **Data:** |
| **Função/Posto:** | **Local:** |

**ENTREVISTA**

As respostas de Sua Excelência são fundamentais para atingir os objetivos da investigação, pelo que se solicita que as mesmas sejam o mais completas possível. As suas respostas irão servir única e exclusivamente como objeto de estudo para a investigação, pelo que lhe é solicitada autorização para efetuar gravação e posterior análise e transcrição das respostas. Se for sua intenção, as mesmas ser-lhe-ão facultadas, juntamente com o trabalho final, assim que o mesmo seja aprovado.

**Questão 1 – Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?**

**Questão 2 – Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?**

**Questão 3 – Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?**

**Questão 4 – Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?**

**Questão 5 – Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?**

**Questão 6** – **Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?**

**Questão 7 - Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?**

**Questão 8 - Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?**

**Questão 9 – Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?**

**Questão 10 – Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?**

Muito obrigado pela sua contribuição.

## APÊNDICE B- Entrevista aos Militares da GNR, Entrevistado 1

**Posto/Função:** Tenente Coronel/Cmdt de Batalhão Academia Militar
**Nome:** Jorge Manuel Sanches e Silva

**Questão 1 – Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?**

Importa referir que, a utilização de meios informáticos para o cometimento de um crime, permite uma abrangência tão vasta que para que pudesse ser conseguida uma resposta objetiva teríamos de avaliar os Despachos finais dos diversos Processos crimes para analisar o enquadramento legal definido pelo titular do inquérito.

No entanto, tendo por base o senso comum, poderemos afirmar que o crime de burla será um dos crimes com expressão no panorama criminal nacional.

**Questão 2 – Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?**

Embora a questão seja mais direcionada para os procedimentos previstos e determinados pelo Departamento de Operações do Comando Operacional, e tendo em conta que neste âmbito a minha experiência é no âmbito da investigação criminal, com base numa análise realizada pela Divisão de Análise e de Investigação Criminal entre 2019 e 2022, considero que devem ser tidos em conta os seguintes aspetos:

1. "*Obter descrição pormenorizada sobre os factos (uma vez que há múltiplas variantes na execução dos factos já detetadas – ver anexo C do RTIC 26/20/RAIC);*
2. *Obter cópia ou impressão do anúncio, identificação da plataforma, com o respetivo ID do anúncio e referência URL do anúncio de venda colocado pela vítima (basta abrir a o anúncio e imprimir a página);*
3. *Perguntar sobre a data e hora da colocação do anúncio e data e hora em que se recebe o contacto pelo agente do crime (frequentemente o contacto é feitos escassas horas após a colocação do anúncio);*
4. *Sobre o suspeito: obter descrição sobre o interlocutor (características: homem, mulher, sotaque, erros ou especificidades na linguagem,*

*nome, localidade ou outras informações – pois ainda que falsas, permitem detetar coincidências noutras narrativas idênticas);*

*5. Acerca da vítima:*

*a. As vítimas devem ser aconselhadas para não apagarem os dados e registos dos telemóveis, nomeadamente as mensagens SMS ou de correio eletrónico que tenham recebido ou enviado;*

*b. De preferência, recolher imagem de todas as mensagens ou de todos os registos que ainda estejam disponíveis nos telefones ou outros dispositivos do queixoso, mormente:*

*i. Números de telefone utilizados pelo agente do crime para contactar o ofendido;*

*ii. Número de telefone inserido em ATM no momento da instalação da aplicação MB WAY (por vezes mencionado como número de referência), indicando no caso de contacto telefónico se o mesmo é pertença da vítima ou do agente do crime;*

*iii. Deve estar descrito o Código PIN (código de 6 dígitos) indicado pelo agente do crime, que foi utilizado pelo denunciante para adesão ao MB WAY;*

*c. Em caso de existirem contactos por outra via, nomeadamente por correio eletrónico, indicar o endereço de e-mail do suspeito;*

*d. Identificação da conta e do(s) cartão(ões) bancário(s) associado(s);*

*e. Identificação do ATM em caso de levantamento por parte do agente do crime (local e entidade): se o ofendido não tiver cancelado o cartão MB, retirar, de imediato, em ATM as informações disponíveis, nomeadamente sobre e entidade e o local de eventual levantamento (na caixa ATM selecionar "consultas" e depois selecionar "operações do cartão na rede Multibanco");*

*f. Obter o extrato de movimentos do cartão – ver se a vítima sabe junto do banco a conta de destino em caso de transferências ou pagamentos;*

*6. Deve estar descrito a hora das operações (levantamento bancário/ transferências) e o local onde foi efetivado o movimento;*

*7. Diligenciar pela preservação das imagens do ATM (para além dos 30 dias a que obriga o n.º 2 do Art.º 13.º do DL n.º 34/2013, de 16 de maio). O período*

*de preservação de imagens, não se deve limitar, à hora referida das operações, mas deverá abranger um período mais alargado;*

*8. Se a vítima efetuou reclamação junto do banco, juntar cópia da mesma;*

*Quando a investigação decorrer na GNR, diligenciar junto do MP o seguinte:*

*1. Solicitação imediata às Operadoras de Telecomunicações da identificação do titular do cartão SIM (número de telefone), bem como todos os equipamentos – IMEI, onde o cartão esteve ativo e restantes números e utilizadores/titulares associados aos números ativos nesse IMEI;*

*2. No caso dos cartões pré-pagos, rogar a indicação do local de venda daquele lote de cartões, para que eventualmente seja possível apurar a existência de imagens captados através dos sistemas de videovigilância ou alguma informação junto do vendedor;*

3. *Se ainda não tiver sido solicitado, diligenciar pela preservação das imagens do ATM (para além dos 30 dias a que obriga o n.º 2 do Art.º 13.º do DL n.º 34/2013, de 16 de maio). O período de preservação de imagens, não se deve limitar, à hora referida das operações, mas deverá abranger um período mais alargado.*"

**Questão 3 – Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?**

As situações criminosas mais identificadas processam-se genericamente da seguinte forma:

• o agente criminoso dos factos escolhe as suas vítimas em plataformas de venda online, procurando aí identificar pessoas que tenham disponibilizado objetos para venda;

• depois, contacta telefonicamente tais pessoas, manifestando a vontade firme de comprar esses objetos e dispondo-se a pagar os mesmos de imediato, mesmo sem os ver e sem ter qualquer garantia de que os mesmos satisfaçam o seu interesse;

• manifesta o intuito de pagar os mesmos por via da aplicação MB WAY;

• em regra, caso a vítima seja conhecedora deste processo de pagamento, o agente dos factos desliga logo a chamada, não voltando a estabelecer qualquer

contacto;

• porém, caso a vítima não conheça a aplicação MB WAY, o agente dos factos desenvolve um processo ardiloso, tendo em vista ter acesso à conta bancária daquela.

O resultado imediato do processo criminoso descrito, possibilita ao agente do crime o acesso à conta bancária da vítima, através da aplicação MB WAY, podendo consultar saldos e movimentos da conta da vítima.

O sistema Multibanco é, nos termos da alínea a) do artigo 2º da Lei do Cibercrime, um sistema informático. Portanto, aceder a uma qualquer parte do sistema Multibanco é suscetível de fazer incorrer o seu autor, sem prejuízo de diferente enquadramento em face das circunstâncias do caso concreto, no crime de acesso ilegítimo (artigo 6º da Lei do Cibercrime).

Para o efeito podem ser usados meios informáticos como telemóveis ou computadores, também.

**Questão 4 – Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?**

O estudo de um perfil para as vítimas não se enquadra na competência da Guarda Nacional Republicana, não obstante, depreende-se das observações às situações criminosas, que as mesmas resultam da falta de conhecimento e da credulidade dos utilizadores.

**Questão 5 – Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?**

Nos termos do respetivo enquadramento legal, Lei do Cibercrime, a Guarda Nacional Republicana não tem competência de investigação neste domínio.

Indiciando-se crimes de acesso ilegítimo ou de falsidade informática, a investigação é da competência Polícia Judiciária, nos termos do Artigo 7º, nº 3, alínea l) da Lei n.º 49/2008, de 27 de agosto, Lei da Organização da Investigação Criminal

Por sua vez, na Guarda Nacional Republicana, a estrutura de investigação criminal com competência encontra-se definida no Despacho N.º 18/14-OG, de 11 de março, com a demais legislação regulamentar e subsidiária:

1. Decreto-Regulamentar N.º 19/2008, de 27NOV;
2. Despacho N.º 1292/2020, de 29JAN, Unidades Orgânicas flexíveis;
3. Despacho N.º 40/20-OG, de 30JAN, Comando Operacional;
4. Despacho N.º 281/19-OG;

5. Etc.

**Questão 6 – Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?**

A investigação de qualquer tipologia criminal tem as suas particularidades e "este tipo de crimes" naturalmente tem as suas. Não quer com isso dizer que possa generalizar ou identificar dificuldades.

**Questão 7 - Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?**

Considero claramente que, de uma forma genérica, a formação dos militares da Guarda é insuficiente para que seja assegurada a resposta institucional que o cidadão, a sociedade e Portugal, esperam de uma instituição secular que procura ser mais "*humana, próxima e de confiança*".

**Questão 8 - Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?**

Ainda não foi criado nenhum curso de investigação para os fenómenos mais complexos, não obstante de já estar pensado e projetado quanto ao seu conteúdo desde 2021.

O desenvolvimento de uma estrutura de investigação criminal para assegurar uma resposta cabal e capaz exige da instituição uma especialização e gestão mais adequada dos seus recursos humanos e um investimento financeiro consecutivo no acompanhamento das evoluções das tendências criminais.

**Questão 9 – Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?**

Resposta idêntica à anterior.

**Questão 10 – Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?**

Considero pertinente uma leitura sobre alguns documentos existentes na Direção de Investigação Criminal, como o "UTILIZAÇÃO FRAUDULENTA DA APLICAÇÃO MB

WAY", Nota Prática PGR n. º 20/2020, 14 de maio, entre muitos outros na Divisão de Análise e de Investigação Criminal, como Normas Técnicas, Instruções Técnicas, Relatórios Temáticos de Informação Criminal e Relatórios de Análise de Informação Criminal.

Muito obrigado pela sua contribuição.

## Apêndice C- Entrevista aos Militares Da GNR, Entrevistado 2

**Posto/Função:** Major/Chefe da SIIC de Vila Real

**Nome: Joni Hélder Gouveia Seabra Ferreira**

**Questão 1 – Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?**

Crime de Burla e Burla Online.

**Questão 2 – Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?**

2- Os constantes da Instrução Técnica difundida pela estrutura de investigação criminal.

"…aspetos a ter em conta aquando da receção da queixa por parte dos militares:

(1) Obter descrição pormenorizada sobre os factos (uma vez que há múltiplas variantes na execução dos factos já detetadas);

(2) Obter cópia ou impressão do anúncio, identificação da plataforma, com o respetivo ID do anúncio e referência URL do anúncio de venda colocado pela vítima (basta abrir a o anúncio e imprimir a página);

(3) Perguntar sobre a data e hora da colocação do anúncio e data e hora em que se recebe o contacto pelo agente do crime (frequentemente o contacto é feitos escassas horas após a colocação do anúncio) (a página impressa do anúncio já contem todos estes elementos. Se possível guardar como ficheiro PDF a página e enviar por correio eletrónico);

(4) Sobre o suspeito: obter descrição sobre o interlocutor (características: homem, mulher, sotaque, erros ou especificidades na linguagem, nome, localidade ou outras informações – pois ainda que falsas, permitem detetar coincidências noutras narrativas idênticas);

(5) Acerca da vítima:

(a) As vítimas devem ser aconselhadas para não apagarem os dados e registos dos telemóveis, nomeadamente as mensagens SMS ou de correio eletrónico que tenham recebido ou enviado;

(b) De preferência, recolher imagem de todas as mensagens ou de todos os registos que ainda estejam disponíveis nos telefones ou outros dispositivos do queixoso, mormente:

1. Números de telefone utilizados pelo agente do crime para contactar o ofendido;

2. Número de telefone inserido em ATM no momento da instalação da aplicação MB WAY (por vezes mencionado como número de referência), indicando no caso de contacto telefónico se o mesmo é pertença da vítima ou do agente do crime;

3. Deve estar descrito o Código PIN (código de 6 dígitos) indicado pelo agente do crime, que foi utilizado pelo denunciante para adesão ao MB WAY;

(c) Em caso de existirem contactos por outra via, nomeadamente por correio eletrónico, indicar o endereço de e-mail do suspeito;

(d) Identificação da conta e do(s) cartão(ões) bancário(s) associado(s);

(e) Identificação do ATM em caso de levantamento por parte do agente do crime (local e entidade): se o ofendido não tiver cancelado o cartão MB, retirar, de imediato, em ATM as informações disponíveis, nomeadamente sobre e entidade e o local de eventual levantamento (na caixa ATM selecionar "consultas" e depois selecionar "operações do cartão na rede Multibanco");

(f) Obter o extrato de movimentos do cartão – ver se a vítima sabe junto do banco a conta de destino em caso de transferências ou pagamentos;

(6) Deve estar descrito a hora das operações (levantamento bancário/ transferências) e o local onde foi efetivado o movimento;

(7) Diligenciar pela preservação das imagens do ATM (para além dos 30 dias a que obriga o n.º 2 do Art.º 13.º do DL n.º 34/2013, de 16 de maio). O período de preservação de imagens, não se deve limitar, à hora referida das operações, mas deverá abranger um período mais alargado;

(8) Se a vítima efetuou reclamação junto do banco, juntar cópia da mesma."

**Questão 3 – Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?**

1. Método A:

a) Atendendo a que os vendedores/prestadores do serviço aceitam o pagamento via MB WAY, propõe o pagamento por esta via;

b) O cidadão aceita receber o valor por MB WAY e o "criminoso/burlão" em vez de selecionar a opção de "Enviar dinheiro" na sua aplicação, seleciona a opção de "Pedir dinheiro";

c) Os cidadãos desconhecendo em pormenor o uso da aplicação e encontrando-se a aguardar o envio do dinheiro, selecionam a opção de aceitar;

d) Sem se aperceberem, acabaram de ser burlados.

2. Método B:

a) Percebendo que os cidadãos desconhecem o uso da aplicação, o "criminoso/burlão" procuram que as vítimas sigam as suas indicações;

b) Desloquem-se a uma caixa Multibanco;

c) Selecionem a Opção MB WAY;

d) Introduzam o seu cartão de multibanco e o código pessoal;

e) Registem o número de telemóvel indicado pelo criminoso, que é o utilizado para a burla;

f) De seguida, introduzam o código de segurança indicado pelo mesmo, criado apenas para efeito pelo criminoso;

g) Em ato continuo, os criminosos passam a assumir o controlo sobre os recursos financeiros disponíveis naquela conta bancária sem que as vítimas se apercebam;

h) Num curto espaço de tempo ficam sem o dinheiro.

**Questão 4 – Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?**

Existe. Na maioria dos casos verifica-se que as vítimas não dominam a aplicação MB WAY.

**Questão 5 – Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?**

Secções de inquéritos/NIC

**Questão 6 – Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?**

Identificação dos autores.

**Questão 7 - Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?**

Sim.

**Questão 8 - Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?**

Não recebem um tipo de formação especifica, no entanto, são difundidas Instruções/orientações sobre a temática, por forma a facilitar todo o trabalho de investigação.

**Questão 9 – Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?**

Sim.

**Questão 10 – Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?**

Nada a acrescentar.

Muito obrigado pela sua contribuição.

## Apêndice D- Entrevista aos Militares da GNR, Entrevistado 3

**Posto/Função:** 1.º Sargento/Chefe do NIC de Vila Real
**Nome:** Paulo Marques Borges Dias

**Questão 1 – Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?**

O crime com maior expressão é a burla informática, nomeadamente através das plataformas digitais como o OLX, o WhatsApp ou o MB Way.

**Questão 2 – Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?**

Para além dos procedimentos comuns no recebimento de uma queixa, entre eles circunstâncias de tempo, lugar e modo.

Então, quando se trata de burlas com utilização de meios informáticos, as vítimas devem indicar a página do anúncio do autor da burla e, para facilitar esta diligência, ser convidada a indicar no computador da própria Guarda abrir a página do *OLX*, *Facebook/Instagram..*, devendo ser realizado um *print screen* que fica desde logo junto aos autos, onde seja visível o URL (*Uniform Rasoure Locador* - vulgarmente conhecido por *Link)*, afigurando-se elemento essencial e indispensável para posteriormente, no decorrer da investigação, se apurar qual o IP da internet que foi usada para a criação da página, para apurar quais os IP's usados nas publicações e comunicações, contribuindo, por vezes, para a descoberta do seu titular.

No caso da página já se encontrar fechada e não ter sido recolhido tal elemento, será muito difícil voltar a obtê-lo, ficando desde logo prejudicada a prova digital, mesmo que seja conhecido o nome da página não é suficiente.

Quando se trata de burla efetuada pela aplicação **MB Way,** que é atualmente a mais recorrente e que teve um grande aumento no período da pandemia, existe alguns procedimentos diferentes, visto que os meios informáticos maioritariamente utilizados são telemóveis e a estes estão associados um número e há por norma uma conversa com o dito "burlão".

Assim é necessário obter descrição sobre o interlocutor (suspeito), nomeadamente as características: homem, mulher, sotaque, erros ou especificidades na linguagem, nome, localidade ou outras informações – pois ainda que falsas, permitem detetar coincidências noutras narrativas idênticas.

As vítimas devem ser aconselhadas para não apagarem os dados e registos dos telemóveis, nomeadamente as mensagens SMS ou de correio eletrónico que tenham recebido ou enviado.

De preferência e caso haja colaboração da vítima, recolher imagem de todas as mensagens ou de todos os registos que ainda estejam disponíveis nos telefones ou outros dispositivos do queixoso, nomeadamente: números de telefone utilizados pelo agente do crime para contactar a vítima; número de telefone inserido em ATM no momento da instalação da aplicação MB WAY; Código PIN (código de 6 dígitos) indicado pelo agente do crime, que foi utilizado pelo denunciante para adesão ao MB WAY; Identificação da conta e do(s) cartão(ões) bancário(s) associado(s); Identificação do ATM em caso de levantamento por parte do agente do crime; diligenciar pela preservação das imagens do ATM; Se a vítima efetuou reclamação junto do banco, juntar fotocópia da mesma.

**Questão 3 – Relativamente ao autor deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?**

Os "burlões" escolhem as suas vítimas através plataformas de venda online, nomeadamente pessoas que tenham disponibilizado objetos para venda, depois, contacta telefonicamente as vítimas, manifestando a vontade firme de comprar esses objetos e dispondo-se a pagar os mesmos de imediato, mesmo sem os ver e sem ter qualquer garantia de estes satisfazem o seu interesse e, no desencadear da conversa, manifesta o intuito de pagar os mesmos por via da aplicação MB WAY e assim está lançado o "isco" para efetuar a burla.

**Questão 4 – Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?**

Na sua maioria as vítimas são vendedores produtos usados nas plataformas OLX, *Facebook, Instagram e outros* (móveis, animais, telemóveis, peças auto, etc) ou compradores (bilhetes ou empréstimos) e que procuram na oferta dos "potenciais

compradores e/ou vendedores" uma forma rápida de escoar o seu produto ou uma aquisição a baixo custo.

O MB WAY surge no seguimento da negociação e como forma de efetuar o pagamento. Quando os lesados ou não têm o serviço ativo ou tendo-o não sabem utilizar devidamente a aplicação, coloca-se numa situação frágil e de grande vulnerabilidade. O burlão, ao se aperceber disto, utiliza o desconhecimento da vítima sobre a funcionalidade e modos de utilização da aplicação em benefício próprio para levar a cabo a burla através deste meio.

**Questão 5 – Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?**

Na GNR, existe Divisão de Investigação de Criminal, onde existem vários órgãos a trabalhar e acompanhar a evolução dos crimes praticados no âmbito digital, especificamente nesta aplicação MB WAY. No entanto, quem leva a cabo as investigações delegadas na Guarda pelo Ministério Publico é essencialmente os NIC - Núcleos de Investigação Criminal e as Equipas de Inquéritos dos Postos Territoriais.

Estas investigações têm a todo o tempo o apoio técnico do NDF - Núcleo Digital Forense, nomeadamente para a prova digital.

**Questão 6 – Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?**

A principal dificuldade é na aquisição da notícia/denúncia, porque, muitas das vezes, têm ausência de elementos essenciais e necessários para a realização de diligências subsequentes que são cruciais para levar a identificação dos autores.

Isto deve-se muito à falta de formação de todos os agentes envolvidos no processo, desde a aquisição da notícia, há investigação, que não reúne factos suficientes para levar a uma acusação, resultando em arquivamento.

**Questão 7 - Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?**

Não, acho que é pouca e tem de ser contínua com partilha de conhecimentos.

**Questão 8 - Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?**

Não, o fenómeno deste tipo de criminalidade é relativamente recente e os militares (investigadores) tem formação para desempenhar funções na Investigação Criminal, no entanto como isto é uma criminalidade muito especifica já justificava haver um curso também ele específico só para este tipo de crimes, à semelhança do que foi feito no passado para a violência doméstica e o tráfico de estupefacientes.

**Questão 9 – Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?**

Os meios nunca são suficientes e a Guarda tem feito um esforço para acompanhar a evolução, nomeadamente com a criação dos NDF - Núcleo Digital Forense.

Agora, com a nova era de tecnologia, nomeadamente do IA (Inteligência artificial), acredito que os "burlões", não tardam em utilizar este meio para praticar os crimes de uma forma mais eficiente e, assim sendo, acho que os meios têm mesmo de ser reforçados, tanto humanos como tecnológicos.

**Questão 10 – Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?**

De uma forma geral foram abordadas as principais questões desta temática, no entanto devia ser abordado também a questão da Lei de Organização da Investigação Criminal - LOIC, que é uma lei que devia ser revista, que de certa forma cria alguns constrangimentos da forma que está atualmente, começando logo pela atribuição do NUIPC.

Muito obrigado pela sua contribuição.

## Apêndice E- Entrevista aos Militares da GNR, Entrevistado 4

**Posto/Função:** 1º Sargento/Academia Militar
**Nome:** Artur Manuel Neves de Pina Robalo

**Questão 1 – Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?**

Os crimes informáticos com maior expressão, tendo em conta a atuação da GNR são o *phising*, ou seja, tentativa de obtenção de informações pessoais através de mensagens fraudulentas como "isco". Temos ainda através da aplicação MB Way, Clonagem de cartões, WhatsApp, Marketplace), Extorsão (Sextortion).

**Questão 2 – Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?**

Recebimento da queixa por parte do militar de atendimento do posto da GNR, onde deverá vir todas as informações pertinentes para a investigação, respondendo às seis perguntas da investigação criminal, ou seja, Quem? Fez o quê? Onde? Como? Quando? E porquê? Seguidamente e dependendo do tipo de crime informático, como por exemplo, pedir à vitima os movimentos bancários fraudulentos, transcrição das mensagens de alguma rede social que tenha servido para iniciar o contacto com a vitima, registar o número e nome da conta para onde o dinheiro foi depositado, caso seja através do OLX, verificar o perfil do burlão no OLX, junto da SIBS apurar onde são efetuados os levantamentos, após o que são levadas a cabo diligências no sentido de apreender imagens de videovigilância existentes estes são alguns procedimentos numa faze inicial de apresentação de queixa por parte do lesado

**Questão 3 – Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?**

Aproveitamento de aliciamento da vítima através de uma venda barata ou compra avultada. O desconhecimento da parte da vítima de algumas plataformas (MBWAY). Por norma estes ilícitos acontecem em situações em que é aceitável socialmente não existir contacto pessoal.

**Questão 4 – Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?**

As vítimas são preferencialmente utilizadores sem muita experiência em sites de compras/vendas (percetível através de anúncios do mesmo utilizador) e/ou utilizadores que vendam por preços mais caros (e ficam entusiasmados com a possibilidade de fazerem um bom negócio).

**Questão 5 – Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?**

Núcleos de Investigação Criminal dos Destacamentos (ou eventuais) e Secções de Inquéritos dos Postos Territoriais.

**Questão 6 – Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?**

A demora das diversas instituições, desde instituições bancárias, informáticas e tribunais. Por norma o atraso deve-se ao facto de as instituições não estarem preparadas para responder ao volume de solicitações em causa.

**Questão 7 - Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?**

Não. Falta muita formação aos militares da Guarda no âmbito de investigação deste tipo de crimes.

**Questão 8 - Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?**

Não. A autoformação e a troca de experiências permite mascarar a falta de formação.

**Questão 9 – Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?**

O nível de investigação e crimes informáticos que, segundo a LOIC, são permitidos à Guarda não exige meios muito avançados de software e/ou meios informáticos.

**Questão 10 – Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?**

A desburocratização na fase da investigação permitiria uma maior celeridade processual, que me parece ser o principal entrave neste tipo de investigações.

Muito obrigado pela sua contribuição.

## Apêndice F- Entrevista aos Militares da GNR, Entrevistado 5

**Posto/Função:** Cabo-Mor/NIC de Lamego
**Nome:** João de Jesus Reis

**Questão 1 – Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?**

Os crimes com recurso a meios informáticos (computadores /Smartphones) que mais ocorrem na ZA da GNR são os crimes de Burla (online) e o Cyberbullying, (onde se incluem a Ameaça, Difamação e extorsão), nas variantes a seguir indicadas:

**Crime de burla online;**

Através da solicitação de pagamento eletrónico fornecendo os burlões as referências multibanco, em websites de compras online que disponibilizam serviços de venda e compra; Através de pagamentos com MBWAY, na qual o Burlão aproveitando a falta de conhecimento deste método pelo(s) lesado(s), oferece ajuda guiando o lesado de forma a que este lhe dê acesso á sua conta bancária ou lhe transfira dinheiro.

**- Crime de Burla online (Bancária);**

Uso do *Phishing*, em que o Lesado recebe um e-mail a simular uma comunicação de uma entidade bancária, levando o mesmo à inserção dos seus dados bancários (passwords/códigos) ficando estes disponíveis ao autor/a da burla.

Uso de *Pharming* em que o Lesado acede de forma enganosa a um servidor falso, digitando numa página que parece fidedigna, os seus dados pessoais (login, números de conta e senhas de acesso, por exemplo) que depois são utilizados para usos fraudulentos.

**Crime de Burla no Comércio eletrónico (E-Commerce) - na compra online de veículos, motores ou outras peças, etc, nas plataformas OLX, Custo Justo e outras;**

Apresentação de um veículo, motor ou outras peças a preço baixo, criando ilusão aos possíveis compradores. Quando o comprador contacta o burlão este diz que está no estrangeiro e solicita transferência bancária para efetuar a reserva e depois transportar o veículo até Portugal. Feita a transferência o Burlão desaparece.

**Leilões na Internet;** Venda de mercadorias a baixo preço, usando websites ou as redes sociais, cujas identidades dos vendedores são falsas e as mercadorias em venda inexistentes.

**Crime de Burla (Amorosa):** Estabelecimento de uma relação amorosa virtual com a vítima, ganhando a sua confiança e subtraindo-lhe códigos de aceso a contas bancárias ou solicitando transferências de quantias monetárias via internet, ou após possuir fotografias íntimas da vítima, fazer chantagem com a sua publicação e extorquir dinheiro.

## Crime de Cyberbullying (englobando ameaças, difamações e extorsão):

Que assenta no comportamento manifestado por um indivíduo ou um grupo de pessoas que, através de meios digitais e de forma deliberada, transmitam mensagens agressivas ou hostis com a intenção de fazer mal ou causar incómodo ao outro.

O assédio virtual pode ter as seguintes formas:

- Telefonemas anónimos repetidos
- SMS com insultos ou mensagens ameaçadoras
- MMS com fotos ou vídeos humilhantes
- Enviar ou apagar e-mails pessoais de outra pessoa
- Publicar imagens alteradas ou comentários jocosos
- Gravar conteúdo inapropriado e publicar online
- Criar um perfil falso e agir em nome da vítima
- Roubo de perfil em rede social
- Bullying nas redes sociais
- Colocar boatos online

**Questão 2 – Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?**

Como procedimento extraordinário, além da cabal narração dos factos e a maior descrição possível do autor do crime e do seu modus operandi (MO) deve-se ainda:

-Identificar a plataforma digital, Rede social ou website utilizado no crime online;

-Obter o consentimento da vítima para pesquisa e recolha de dados no seu computador/smartphone;

-Recolher todos os dados possíveis do meio informático /computador ou smartphone da vítima (nº. de telemóvel do suspeito, vídeos, fotografias, SMS enviadas/recebidas, emails enviados/recebidos, conversas em chats e nºs de contas bancárias que o suspeito indique; (para o efeito fazer print screen ou download para Pen Drive e juntar aos autos);

- Caso se apreenda durante a investigação o computador/smartphone do suspeito, deve-se procurar obter as passwords de acesso e posteriormente enviar os equipamentos para o NTP (Núcleo Técnico Pericial da GNR) para o devido exame;

- Pesquisar na internet se o website, ou o perfil do suspeito ainda continua ativo;

- Pesquisar se há conhecimento de outras burlas com o mesmo MO na GNR e outros OPC;

- Elabora Relatório de Pesquisa e difundir ao dispositivo para possível identificação do suspeito ou do seu MO;

**Questão 3 – Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?**

A técnica principal usada pelo Burlão é a astucia e consiste primariamente na colocação para venda na internet, a preço reduzido de um artigo, ou na proposta de algo muito vantajoso para a vítima estabelecendo para o efeito uma relação de confiança com a mesma, o que lhe permitirá pôr em prática o seu plano. O uso generalizado de smartphones e computadores com acesso à internet veio possibilitar a interação pessoal á distancia, sem a presença do outro e sem se ver in loco a mercadoria em comércio, o que ainda mais potenciou o aumento deste e o seu maior êxito.

**Questão 4 – Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?**

Como nas demais burlas, a burla através de meio informático aponta a vítimas com um perfil de vulnerabilidade, isto por força da sua pouca literacia digital, idade, pouca instrução académica, deficiência ou doença;

De referir que a vítima muitas vezes julga estar a ter vantagem ou a ser até mais inteligente que o burlão, sendo um fator que a leva a concordar com o negócio proposto.

**Questão 5 – Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?**

Geralmente, estes inquéritos são encaminhados para os Núcleos de investigação Criminal (NIC), os quais desenvolvem diligências com o auxílio dos NTP (Núcleos Técnicos Forenses da GNR e por vezes do LPC da Polícia Judiciária.

Quando as queixas integram factos tipificados como Burla Informática (pena superior a 5 anos) são enviados ao Mº. Pº. para delegação de competência de investigação, pois serão da competência da PJ.

**Questão 6 – Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?**

As maiores dificuldades encontradas a respeito dos crimes através de meios informáticos, acontece na localização do infrator, na qual o investigador (GNR) na sua maioria, não contém equipamentos, softwares apropriados e carece de profissionais especializados para rastrear os fatos, ficando ausente a autoria e a materialidade, que são provas essenciais para a constituição do crime.

**Questão 7 - Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?**

Pessoalmente a minha resposta é não. A informática evolui diariamente e a formação dos militares é mínima e os equipamentos poucos atuais e carecem de licenças de software em número suficiente para determinadas pesquisas. De referir que as legislações em vigor não acompanham a evolução deste tipo de crime.

**Questão 8 - Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz?**

Nos Núcleos de Investigação Criminal não tem havido ultimamente quaisquer formações nesta área, socorrendo-se os investigadores dos elementos dos NTP, no entanto estes militares apenas fazem as pesquisas nos equipamentos apreendidos e não fazem a correlação dos dados que extraem.

**Questão 9 – Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área?**

Existe quanto a mim uma falta gritante de meios para investigar esta tipologia de crime, sejam eles militares especializados ou meios informáticos de pesquisa**.**

Seria uma boa ajuda alguns Engenheiros informáticos a trabalhar com a Guarda dada a complexidade que esta investigação apresenta.

**Questão 10 – Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo?**

Acrescento ainda que as dificuldades de investigar estes crimes esbarram ainda na quase impossibilidade de se poderem obter interceções em tempo real às redes sociais (Facebook, WhatsApp, Instagram etc.). De referir que mesmo de comunicações efetuadas no passado é muito difícil obter a colaboração destas empresas, pois estão sediadas em países terceiros e a legislação nacional não tem força de lei para se conseguir tal desiderato, o que cria uma imagem de impunidade face a estes crimes.

Muito obrigado pela sua contribuição.

## Apêndice G- Quadro-Relação para a Elaboração das Entrevistas

| Questão Central | Questões Derivadas | Questões para a entrevista |
|---|---|---|
| **QP. – De que forma é conduzida uma investigação de crimes através de meios eletrónicos pela Guarda Nacional Republicana?** | QD.1- Quais são os tipos de crimes realizados através de meios eletrónicos com maior expressão em Portugal? | QE.1- Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS?<br><br>QE.2- Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way?<br><br>QE.3- Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?<br><br>QE.4- Existe algum perfil estabelecido para as vítimas mais |

| | | |
|---|---|---|
| | | comuns de burlas através de meios eletrónicos? |
| | QD.2- Quais são estruturas dentro da GNR Que fazem a investigação deste tipo de crimes? | QE.5- Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais? |

| | | |
|---|---|---|
| | QD.3- Quais os principais obstáculos colocados à investigação deste tipo de crimes? | QE.6- Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes? |
| | | QE.7- Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos? |
| | | QE.8- Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz? |
| | | QE.9- Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área? |

**Quadro 1- Quadro-Relação para a Elaboração das Entrevistas**

**Fonte: Elaboração Própria**

# Apêndice H- Apresentação e Análise das Respostas às Entrevistas

## 1. Apresentação e análise da questão nº1

| Questão nº1: Tendo em conta a área de atuação da GNR, quais são os tipos de crime com recurso a meios informáticos com maior expressão, e que, devido a esse facto exijam uma maior atenção por parte desta FS? | |
|---|---|
| **Nº** | **Resposta** |
| **E1 (TC)** | • Burla |
| **E2 (Maj)** | • Burla<br>• Burla Online |
| **E3 (1º Dias)** | • Burla Informática, através de plataformas digitais como o OLX, WhatsApp ou MB Way |
| **E4 (1º Robalo)** | • *Phishing*<br>• Burlas através de aplicações como MB Way, WhatsApp, Marketplace<br>• Extorsão (*Sextortion*) |
| **E5 (CbMor Reis)** | • Burla Online<br>• Cyberbullying (Ameaça, Difamação e Extorsão) |

**Quadro 2 – Apresentação e análise da questão nº1**

**Fonte: Elaboração Própria**

## 2. Apresentação e análise da questão nº2

| Questão nº2: Quais são os procedimentos a tomar aquando da receção de uma queixa de burla efetuada através de um meio eletrónico, por exemplo utilizando plataformas digitais como o OLX, o WhatsApp ou o MB Way? | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • Para além dos procedimentos comuns aquando o recebimento de uma queixa pelos militares da Guarda<br>• Obter descrição pormenorizada sobre os factos<br>• Obter cópia ou impressão do anúncio, identificação da plataforma com o respetivo ID do anúncio e referência URL do anúncio da venda colocado pela vítima |

| | |
|---|---|
| | • Questionar a data e hora da colocação do anúncio e data e hora de recção do contacto pelo agente do crime<br>• Obter a descrição do suspeito (ex. género, possível sotaque, especificidades linguísticas, nome, localidade ou outras informações, que apesar de provavelmente falsas, permitem detetar coincidências noutras narrativas idênticas<br>• Relativamente à vítima, não apagar dados e registos do telemóvel, nomeadamente mensagens SMS ou correio eletrónico que tenham recebido ou enviado; recolher imagem de todas as mensagens ou registos que tenham sido feitos através dos equipamentos eletrónicos; em caso de existirem contactos por outras vias, nomeadamente correio eletrónico, indicar qual o endereço eletrónico do suspeito; identificação da conta e cartão bancário associado; identificação do ATM em caso de levantamento por parte do agente do crime; obter o extrato dos movimentos do cartão; diligenciar pela preservação das imagens do ATM; se existir queixa junto ao banco da vítima, anexar uma cópia<br>• Solicitação da identificação do titular do cartão SIM junto das Operadoras de Telecomunicações, bem como todos os equipamentos IMEI onde o cartão esteve inserido e titulares associados aos números ativos desse IMEI |
| **E2** | • Resposta idêntica |
| **E3** | • Resposta idêntica |
| **E4** | • Resposta idêntica |
| **E5** | • Resposta idêntica |

**Quadro 3 – Apresentação e análise da questão nº2**

**Fonte: Elaboração Própria**

## 3. Apresentação e análise da questão nº3

| **Questão nº3: Relativamente ao ator deste tipo de crime, que técnicas são as mais utilizadas para efetuar uma burla, e de que forma podemos ligar este crime aos meios informáticos como telemóveis ou computadores?** | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • Escolher as vítimas através de plataformas de compra e venda de produtos online<br>• Contactar telefonicamente as vítimas selecionadas<br>• Manifestar o intuito de efetuar o pagamento através de plataformas de pagamento eletrónico (ex. MB Way)<br>• Desenvolvimento de um processo ardiloso para levar ao engano a vítima |
| **E2** | • **1º método:** propor pagamento através de MB Way; o criminoso/burlão seleciona a opção de "pedir dinheiro" em vez de "enviar dinheiro"; os cidadãos desconhecendo o funcionamento da aplicação ao pormenor aceitam a opção e acabam por ser burlados<br>• **2º método:** devido ao desconhecimento do uso de aplicações como o MB Way, os criminosos/burlões procuram que as vítimas sigam as suas instruções; estes deslocam-se a uma caixa multibanco e selecionam a opção "MB Way", introduzindo o seu cartão bancário e código pessoal; registam o número de telemóvel indicado pelo criminoso e de seguida introduzem o código de segurança indicado pelo burlão para efetivar a burla; deste modo o burlão passa a ter acesso aos recursos financeiros daquela conta bancária, sem que as vítimas se |

| | |
|---|---|
| | apercebam, ficando sem dinheiro num curto espaço de tempo |
| **E3** | • A escolha das vítimas é feita através de plataformas de venda online, nomeadamente pessoas que tenham disponibilizado objetos para venda<br>• Contacto do burlão manifestando a intenção de comprar o produto que está a ser vendido<br>• Manifestar o intuito de efetuar o pagamento através da aplicação MB Way, e a partir daqui efetuam a burla enganando as vítimas |
| **E4** | • Aliciamento da vítima através de uma venda barata ou compra avultada<br>• Aproveitar o desconhecimento da vítima na utilização de plataformas como o MB Way para efetuar a burla |
| **E5** | • A principal técnica é astucia, numa primeira fase colocando algo para venda, numa plataforma de vendas online, a um preço reduzido, ou propondo algo muito vantajoso para a vítima, estabelecendo uma relação de confiança por parte da mesma |

**Quadro 4 – Apresentação e análise da questão nº3**

**Fonte: Elaboração Própria**

## 4. Apresentação e análise da questão nº4

| **Questão nº4: Existe algum perfil estabelecido para as vítimas mais comuns de burlas através de meios eletrónicos?** | |
|---|---|
| Nº | **Resposta** |
| **E1** | • Falta de conhecimento da utilização de meios eletrónicos<br>• Credulidade dos utilizadores |
| **E2** | • Cidadãos que não dominem aplicações como o MB Way |
| **E3** | • Vendedores de produtos em plataformas como OLX, Marketplace, etc.., e que procuram ofertas feitas por potenciais |

| | |
|---|---|
| | compradores, que ao se aperceberem da falta de conhecimento dos vendedores relativamente às plataformas que estão a utilizar, os induzem em erro, colocando-os em situações de fragilidade e vulnerabilidade |
| **E4** | • Utilizadores sem muita experiência em sites de compra e venda de produtos online<br>• Utilizadores que vendam por preços mais caros nesses mesmos sites |
| **E5** | • Cidadãos com perfil de vulnerabilidade, por força da sua pouca literacia digital, idade, baixa instrução académica, deficiência ou doença |

**Quadro 5 – Apresentação e análise da questão nº4**

**Fonte: Elaboração Própria**

## 5. Apresentação e análise da questão nº5

| **Questão nº5: Dentro da GNR, quais são as estruturas que fazem a investigação dos crimes de burla com recurso a meios digitais?** | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • No caso de estes crimes representarem crimes de acesso ilegítimo ou falsidade informática, a competência é da PJ<br>• A estrutura de IC da GNR com competência para investigar burlas online encontra-se definida no Despacho N.º 18/14-OG, de 11 de março, bem como na legislação regulamentar subsidiária |
| **E2** | • Secções de inquéritos<br>• NIC |
| **E3** | • NIC<br>• Equipas de inquéritos das Secções de inquéritos dos PTer<br>• NDF quando é necessário apoio técnico |
| **E4** | • NIC<br>• Secções de inquéritos |

| | |
|---|---|
| **E5** | • NIC<br>• NTP<br>• Secções de inquéritos<br>• LPC da PJ (quando necessário)<br>• No caso de as queixas tiverem pena superior a 5 anos, os processos são enviados ao MP, uma vez que será competência da PJ |

**Quadro 6 – Apresentação e análise da questão nº5**

**Fonte: Elaboração Própria**

## 6. Apresentação e análise da questão nº6

| **Questão nº6: Quais são as maiores dificuldades que se colocam à investigação deste tipo de crimes?** | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • Todos os tipos criminais possuem as suas particularidades, tal como este tipo de crime tem as suas, no entanto não é correto generalizar ou identificar dificuldades |
| **E2** | • Identificação dos autores |
| **E3** | • Aquisição da notícia de crime, porque, muitas das vezes há ausência de elementos essenciais e necessários para a realização de diligências subsequentes que são cruciais para a identificação dos autores |
| **E4** | • Demora das diversas instituições, desde instituições bancárias, informáticas e tribunais, uma vez que, por norma, este tipo de instituições não se encontram preparadas para responder ao volume de solicitações existentes |
| **E5** | • Localização do infrator, uma vez que na maioria dos casos, os investigadores não possuem equipamentos apropriados e carece de profissionais especializados para rastrear os factos, ficando ausente a autoria e a materialidade, que são provas |

| | |
|---|---|
| | essenciais para a constituição de crime |

**Quadro 7 – Apresentação e análise da questão nº6**

**Fonte: Elaboração Própria**

## 7. Apresentação e análise da questão nº7

| **Questão nº7: Considera que a formação dos militares da Guarda é suficiente para os habilitar a trabalhar neste tipo de processos?** | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • De uma forma genérica, e não só neste tipo de crimes, nota-se que a formação dos militares da Guarda é insuficiente para que seja assegurada uma resposta institucional que o cidadão, a sociedade e Portugal esperam de uma instituição secular que procura ser mais "humana, próxima e de confiança" |
| **E2** | • Sim |
| **E3** | • Pouca e deve ser contínua, com partilha de conhecimentos |
| **E4** | • Falta muita formação aos militares da Guarda no âmbito deste tipo de crimes |
| **E5** | • Não, a informática evolui diariamente e a formação dos militares é mínima, e os equipamentos atuais carecem de licenças de *software* em número suficiente para determinadas pesquisas; além disto, a legislação em vigor não acompanha a evolução deste tipo de crimes |

**Quadro 8 – Apresentação e análise da questão nº7**

**Fonte: Elaboração Própria**

## 8. Apresentação e análise da questão nº8

| Questão nº8: Os militares que fazem a investigação deste tipo de crimes recebem algum tipo de formação específica que os capacite a fazê-lo de forma mais eficiente e eficaz? | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • **Apesar de ainda não ter sido criado qualquer curso específico relativamente a este fenómeno criminal, e fenómenos mais complexos, este já está a ser pensado e projetado quanto ao seu conteúdo desde 2021** |
| **E2** | • Não têm formação específica, no entanto são difundidas instruções/orientações sobre a temática, por forma a facilitar todo o trabalho de investigação |
| **E3** | • Este tipo de fenómeno criminal é relativamente recente, e os investigadores possuem apenas formação para a IC no seu sentido amplo, como este é um tema muito específico, justifica-se que haja um curso também ele específico para este tipo de crimes, à semelhança do que acontece com os crimes de violência doméstica e tráfico de estupefacientes |
| **E4** | • Não, a autoformação e a troca de experiências vão permitindo aos militares mascarar a falta de formação |
| **E5** | • Nos NIC não tem havido formações nesta área ultimamente, sendo que os militares se socorrem de elementos do NTP, no entanto estes apenas realizam pesquisas nos equipamentos apreendidos, não fazendo a correlação dos dados que extraem |

**Quadro 9 – Apresentação e análise da questão nº8**

**Fonte: Elaboração Própria**

## 9. Apresentação e análise da questão nº9

| Questão nº9: Considera que os meios/software que a Guarda possui são os necessários e adequados para a investigação deste tipo de crimes ou, por outro lado, existe uma falta de meios nesta área? | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • O desenvolvimento de uma estrutura de IC para assegurar uma resposta cabal e capaz, exige da instituição uma especialização e gestão mais adequada dos seus recursos quer humanos quer materiais, para além de um investimento financeiro consecutivo no acompanhamento das evoluções das tendências criminais |
| **E2** | • Sim |
| **E3** | • Os meios nunca são suficientes, no entanto a GNR tem feito um esforço no sentido de acompanhar a evolução criminal, como a criação do NDF<br>• O surgimento de novas tecnologias, como a Inteligência Artificial, não tarda a ser utilizado pelos burlões para praticar os crimes de uma forma mais eficiente, e assim sendo, os meios da Guarda devem ser reforçados, quer tecnológicos como humanos |
| **E4** | • O nível de investigação e crimes informáticos que são permitidos à Guarda investigar, segundo a LOIC, não exige meios muito avançados de *software*/informáticos |
| **E5** | • Existe uma falta gritante de meios para realizar a investigação deste tipo de criminalidade, sejam eles militares especializados, ou meios informáticos de pesquisa<br>• Seria uma boa medida, a Guarda poder trabalhar com alguns engenheiros Informáticos, dada a complexidade que esta investigação apresenta |

**Quadro 10 – Apresentação e análise da questão nº9**

**Fonte: Elaboração Própria**

## 10. Apresentação e análise da questão nº10

| Questão nº10: Após tudo o que foi questionado, pode acrescentar mais esclarecimentos sobre o tema que ache relevante abordar no estudo? | |
|---|---|
| **Nº** | **Resposta** |
| **E1** | • Leitura de documentos tais como "Utilização Fraudulenta da Aplicação MB Way" |
| **E2** | • Nada a acrescentar |
| **E3** | • Revisão da LOIC, uma vez que cria alguns constrangimentos da forma como está atualmente, começando logo pela atribuição de NUIPC |
| **E4** | • Desburocratização ma fase de investigação permitiria uma maior celeridade processual |
| **E5** | • Dificuldades em se poder obter interseções em tempo real às redes sociais como o Facebook, Instagram, etc.<br>• Mesmo tratando-se de comunicações passadas, a colaboração destas empresas é difícil de obter, uma vez que estão sediadas em países terceiros e a legislação nacional não tem força de lei para se conseguir tal desidrato, o que cria uma imagem de impunidade face a estes crimes |

**Quadro 11 – Apresentação e análise da questão nº10**

**Fonte: Elaboração Própria**