

ACADEMIA MILITAR

Crimes em ambiente digital – Investigação da GNR para a obtenção de prova

Autor: Aspirante Aluno de GNR Cavalaria Miguel Ângelo Trindade Mateus

Orientador: Tenente-Coronel de GNR Infantaria Paulo Jorge Soares dos Santos

Coorientador: Major de GNR Infantaria Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares, na especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, setembro de 2016



ACADEMIA MILITAR

Crimes em ambiente digital – Investigação da GNR para a obtenção de prova

Autor: Aspirante Aluno de GNR Cavalaria Miguel Ângelo Trindade Mateus

Orientador: Tenente-Coronel de GNR Infantaria Paulo Jorge Soares dos Santos

Coorientador: Major de GNR Infantaria Tiago Lourenço Lopes

Mestrado Integrado em Ciências Militares, na especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, setembro de 2016

EPÍGRAFE

*“The farther backward you can look,
the farther forward you will see”.*

Winston Churchill

AGRADECIMENTOS

Uma investigação desta natureza não é possível de ser concretizada sem a ajuda e apoio de um grupo de intervenientes. Desta forma gostaria de prestar aqui os meus sinceros agradecimentos àqueles que me deram o apoio mais direto durante a realização da investigação.

Em primeiro lugar, ao Sr. Tenente Coronel Soares dos Santos e ao Sr. Major Lourenço Lopes, que assumiram a orientação da investigação e estiveram a todo o momento disponíveis para auxiliar, sendo este auxílio decisivo para a concretização do trabalho.

À minha família e namorada, que tanto me deram o apoio moral e sentimental durante o período da realização da investigação.

Ao Sr. Dr. Pedro Verdelho, Sr. Dr. Rui Cardoso, Sr. Dr. Carlos Pinho, Sr. Coronel Vivas, Sr. Major Botas e Sr. Major Machado, pela concessão das entrevistas que foram fundamentais para a realização do trabalho de campo.

Aos militares do Núcleo Técnico Pericial do Comando Territorial de Coimbra, Sr. Cabo Rodrigues e Sr. Guarda Principal Cardoso, não só pela entrevista concedida, mas também pelo esclarecimento de todas as dúvidas acerca da realização dos exames forenses.

A todos os chefes de núcleos de investigação criminal que fizeram parte da amostra dos questionários.

Ao Sr. Tenente Coronel Machado, pelo auxílio que prestou ao estabelecer o contacto com algumas das entidades entrevistadas.

Por último, não respeitando só à concretização da tese, porque a tese é apenas o culminar de um período de cinco anos de formação, quero agradecer aos meus camaradas de curso por me apoiarem neste longo percurso, a Academia Militar é um estabelecimento de ensino superior militar rigoroso e o apoio e entreaajuda entre camaradas foi essencial para o terminar com sucesso.

RESUMO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada está subordinado ao tema “Crimes em ambiente digital – Investigação da GNR para a obtenção de prova”. O tema enunciado tem como finalidade fazer uma análise da investigação criminal da GNR, no que diz respeito à obtenção de prova digital, em inquéritos delegados pela Autoridade Judiciária. Como objetivo geral pretende-se determinar a importância da prova digital para a investigação criminal da GNR. A investigação tem ainda objetivos específicos como a determinação das capacidades e dificuldades das vertentes operativa e criminalística para a obtenção de prova digital e também a determinação dos principais tipos de crime que se suportaram neste tipo de prova.

Ao nível das bases lógicas, a presente investigação apoia-se no método hipotético-dedutivo, como tal, o ponto de partida é a conceção das questões de investigação, respetivos objetivos e hipóteses de investigação. No que diz respeito às técnicas de recolha de dados, a presente investigação é apoiada em conteúdo documental, entrevistas e questionários. A análise e discussão dos resultados obtidos permite tecer as conclusões do trabalho que, por sua vez, permitem verificar a veracidade das hipóteses formuladas na fase inicial da investigação.

Como principais resultados conseguimos constatar que a prova digital é um tipo de prova que deve ser priorizada para os inquéritos podendo ser obtida num grande espectro de tipologias criminais que são da competência da GNR, em matéria de investigação criminal. Concluimos também que a Guarda ainda tem uma grande margem de progressão até estar completamente capacitada para a obtenção de prova digital, ainda assim, estão a ser desenvolvidos esforços e competências nesse sentido, sendo que alguns Comandos Territoriais se encontram mais desenvolvidos nesta matéria.

Palavras-chave: Autoridade Judiciária, Investigação Criminal da Guarda Nacional Republicana e Prova Digital.

ABSTRACT

The present Final Scientific Report of the Applied Investigation Work has been entitled as “Digital environment crimes – GNR’s investigation towards evidence collection”. This scientific research was able to analyse GNR’s criminal investigation, concerning to digital evidence collection, by Judicial Authority inquiries. The main objective aims to determine the importance of digital evidence for criminal investigation of the GNR. Specific objectives include not only determining the strengths and difficulties of both operative and criminalistic aspects for obtaining digital evidence, but also the determination of the main types of crime that use digital evidence.

In terms of the logical research bases, this research relies on hypothetical-deductive method, as so the starting point is the design of the research questions, respective objectives and research hypotheses. As far as data collection techniques are concerned, the present investigation is supported on official documents, questionnaires and interviews. The analysis and discussion of the results enable to reach the conclusions of the work which, in turn, verify the veracity of those previous formulated hypothesis.

The main results show that digital evidence is a type of evidence that should be prioritized for investigation once it can be obtained in a wide spectrum of criminal typologies which are GNR’s competence. We also conclude that the GNR still has great room for improvement to be fully able to obtain digital evidence, yet there are already efforts and skill development in order to achieve this goal, as well as some territorial commands that are more developed on this subject.

Keywords: Judicial Authority, GNR’s Criminal Investigation and Digital Evidence.

ÍNDICE GERAL

EPÍGRAFE	2
AGRADECIMENTOS.....	iii
RESUMO	iv
ABSTRACT	v
ÍNDICE DE TABELAS	viii
ÍNDICE DE FIGURAS	ix
LISTA DE APÊNDICES.....	x
LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS.....	xi
INTRODUÇÃO	1
CAPÍTULO 1 ENQUADRAMENTO TEÓRICO	3
1.1. Investigação Criminal na GNR	3
1.2. Prova Penal	5
1.3. Prova digital	8
1.4. Cibercrime e crimes em ambiente digital	16
CAPÍTULO 2 METODOLOGIA E PROCEDIMENTOS	18
2.1. Introdução	18
2.2. Método de Abordagem e Bases Lógicas	18
2.3. Métodos e Técnicas de Recolha de Dados	19
2.3.1. Análise Documental.....	19
2.3.2. Entrevistas	20
2.3.2.1. Caracterização da Amostra	21
2.3.3. Inquéritos por Questionário	23
2.3.3.1. Caracterização da Amostra	23
CAPÍTULO 3 APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS.....	25
3.1. Introdução	25
3.2. Análise Documental	25
3.3. Análise das Entrevistas	30
3.3.1 Análise de Conteúdo à Questão 1	30
3.3.2. Análise de Conteúdo à Questão 2	31
3.3.3. Análise de Conteúdo à Questão 3	34
3.3.4. Análise de Conteúdo à Questão 4	35
3.3.5. Análise de Conteúdo à Questão 5	36

3.3.6.	Análise de Conteúdo à Questão 6	37
3.3.7.	Análise de Conteúdo à Questão 7	38
3.3.8.	Análise de Conteúdo à Questão 8	39
3.3.9.	Análise de Conteúdo à entrevista efetuada ao NTP Coimbra.....	40
3.4.	Análise dos Questionários.....	42
CONCLUSÕES E RECOMENDAÇÕES		47
BIBLIOGRAFIA		52

ÍNDICE DE TABELAS

TABELA 1: CARACTERIZAÇÃO DOS ENTREVISTADOS.....	22
TABELA 2: EXAMES E PERÍCIAS NO ÂMBITO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO.....	25
TABELA 3: EXAMES FORENSES NO ÂMBITO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO, EFETUADOS PELA GNR.	25
TABELA 4: TIPOS DE CRIME INVESTIGADOS NOS INQUÉRITOS JUDICIAIS.	27
TABELA 5: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º1.....	31
TABELA 6: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º 2.....	33
TABELA 7: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º3.....	35
TABELA 8: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º4.....	36
TABELA 9: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º5.....	37
TABELA 10: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º6....	38
TABELA 11: ANÁLISE QUALITATIVA E QUANTITATIVA DAS RESPOSTAS À QUESTÃO N.º7....	38
TABELA 12: ANÁLISE QUALITATIVA E QUANTITATIVA DA RESPOSTAS À QUESTÃO N.º8.	40
TABELA 13: NECESSIDADE DE OBTENÇÃO DE PD EM INQUÉRITOS POR TIPO DE NÚCLEO IC.	43

ÍNDICE DE FIGURAS

FIGURA 1: PERCENTAGEM DE INQUÉRITOS COM DISPOSITIVOS ELETRÓNICOS NO NTP DA GNR POR ÓRGÃO POLICIAL OU JUDICIAL QUE REGISTOU A NOTÍCIA DE CRIME.	28
FIGURA 2: QUANTIDADE DE INQUÉRITOS CRIME POR UNIDADE DA GNR E SEF QUE NECESSITARAM DE RECOLHER PROVA POR VIA DE EXAMES FORENSES REALIZADOS NO NTP DA GNR	29

LISTA DE APÊNDICES

APÊNDICE A – Guião de Entrevista (Magistrados do MP e Oficiais da GNR)	I
APÊNDICE B – Guião de Entrevista (NTP Coimbra).....	II
APÊNDICE C – Questionários núcleos IC	III
APÊNDICE D – Tipos de crime investigados nos inquéritos judiciais	V
APÊNDICE E – Tipos de núcleo IC na origem dos pedidos de exame forense para obtenção de PD	VI
APÊNDICE F – Lista de segmentos definidos.....	VII
APÊNDICE G – Análise das entrevistas.....	X
APÊNDICE H – Transcrição entrevista NTP Coimbra.....	XIX
APÊNDICE I – Respostas à questão 1 do grupo 3 do questionário	XXII
APÊNDICE J – Respostas à questão 2 do grupo 3 do questionário.....	XXII

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

- ADB** – Android Debug Brigde
AJ – Autoridade Judiciária
AM – Academia Militar
art. – Artigo
cmdt – Comandante
CNCS – Centro Nacional de Cibersegurança
CO – Comando Operacional
CPP – Código de Processo Penal
CRP – Constituição da República Portuguesa
Cfr – Conforme
CTer – Comando Territorial
DIAP – Departamento de Investigação e Ação Penal
DL – Decreto Lei
DTer – Destacamento Territorial
GNR – Guarda Nacional Republicana
HI – Hipótese de Investigação
IACISIS – International Association of Computer Investigative Specialists
IOCE – International Organization for Criminal Digital Evidence
ISP – Internet Service Provider
JIC – Juiz de Instrução Criminal
LC – Lei do Cibercrime
MCP – Medidas Cautelares e de Polícia
MOP – Meios de Obtenção de Prova
MP – Ministério Público
n/d – Não determinado
NAO – Núcleo de Apoio Operativo
NAT – Núcleo de Apoio Técnico
NAIIC – Núcleo de Análise de Informações e Informação Criminal
NAIVE – Núcleo de Investigação e de Apoio a Vítimas Específicas
NIC – Núcleo de Investigação Criminal
NICAV – Núcleo de Investigação de Crimes e Acidentes de Viação

NICCO – Núcleo de Investigação de Crimes e Contraordenações
NICCOA – Núcleo de Investigação de Crimes e Contraordenações Ambientais
NTP – Núcleo Técnico-Pericial
NUIPC - Número Único de Identificador de Processo Crime
OE – Objetivo específico
OPC – Órgão de Polícia Criminal
PD – Prova Digital
PGR – Procuradoria Geral da República
PJ – Polícia Judiciária
PTer – Posto Territorial
QP – Questão de partida
RAFD – Repartição de Análise Forense Digital
RCFTIA – Relatório Científico Final do Trabalho de Investigação Aplicada
SEF – Serviço de Estrangeiros e Fronteiras
Sgts – Seguintes
SIC – Secção de Investigação Criminal
SIIC – Secção de Informações e Investigação Criminal
SWGDE – Scientific Working Group on Digital Evidence
TIC – Tecnologias de Informação e Comunicação
UAF – Unidade de Ação Fiscal
UI – Unidade de Intervenção
USB – Universal Serial Bus

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA) insere-se no plano curricular do mestrado em ciências militares na especialidade de segurança. A investigação encontra-se subordinada ao tema: “*Crimes em ambiente digital – Investigação da GNR para a obtenção de prova*”. O tema enunciado tem como finalidade fazer uma análise da investigação criminal (IC) da Guarda Nacional Republicana (GNR), mais concretamente, no que diz respeito à obtenção de prova digital (PD), em inquéritos delegados pela Autoridade Judiciária (AJ).

Hoje em dia, com os avanços tecnológicos, grande parte da população tem acesso às Tecnologias de Informação e de Comunicação (TIC), usando as mesmas no seu dia-a-dia de forma comum e disseminada. A este crescente uso das TIC surge associadamente o cometimento de ilícitos criminais em ambiente digital ou onde as TIC possam conter vestígios do cometimento desses mesmos crimes. Assim, há um grande conjunto de crimes que podem ser cometidos em ambiente digital ou que possam implicar PD, não se resumindo unicamente à cibercriminalidade. Segundo o Plano de Ação do Ministério Público 2015-2016, a necessidade de obter elementos de prova em ambiente digital é partilhada por todas as jurisdições, com maior ênfase nas áreas criminais e de família e menores. O presente trabalho foca-se exclusivamente na área da IC da GNR abordando as vertentes operativa e criminalística. Sendo esta uma área bastante atual e emergente, requer uma adaptação da GNR, acompanhando assim a evolução da sociedade e dos fenómenos criminais. Posto isto, é bastante útil e pertinente que, para um órgão de polícia criminal (OPC) de competência genérica, como a GNR, sejam efetuados estudos sobre este tema.

Como objetivo geral da investigação, pretende-se determinar qual a importância da PD nos inquéritos delegados pelo Ministério Público (MP) à GNR e, para cumprir este objetivo, foi formulada a seguinte questão de partida (QP): “*Qual a importância da prova digital nos inquéritos delegados pelo Ministério Público à GNR?*”.

Para apoiar a resposta à QP, foram definidas três questões derivadas (QD):

- QD1: Quais as capacidades e dificuldades dos núcleos IC na obtenção de PD?
- QD2: Quais as capacidades e dificuldades da componente criminalística da GNR, na realização de exames forenses, para extração de PD?
- QD3: Quais os principais tipos de crime, da competência de investigação da GNR, associados à PD?

As QD têm os seguintes objetivos específicos (OE):

- OE1: Determinar as capacidades e dificuldades dos núcleos IC na obtenção de PD;
- OE2: Determinar as capacidades e dificuldades da componente criminalística da GNR na realização de exames forenses, para extração de PD;
- OE3: Determinar quais os principais tipos de crime, da competência de investigação da GNR, associados à PD.

Para cada OE foi levantado uma hipótese de investigação (HI):

- HI1: Os núcleos IC não orientam a sua atividade para obtenção de PD;
- HI2: A vertente criminalística da GNR tem capacidade para fazer a recolha de prova em qualquer dispositivo eletrónico;
- HI3: Os principais tipos de crime associados à PD são a violência doméstica contra cônjuges ou análogos e o tráfico de droga.

O presente RCFTIA está redigido e articulado de acordo com as normas estipuladas pela Academia Militar (AM), mais precisamente pela Norma de Execução Permanente (NEP) 520/4.^a (AM, 2015) e pela NEP 522/1.^a (AM, 2016). Deste modo, no que à parte textual diz respeito, encontra-se subdividido em: Introdução, onde é feita a apresentação do tema, a sua justificação e são também dadas a conhecer as questões de investigação levantadas, bem como a estrutura do RCFTIA; Capítulo 1 - Revisão de Literatura, onde é dado a conhecer o atual estado da arte sobre os principais conceitos relacionados com o tema; Capítulo 2 - Metodologia e Procedimentos, este é o capítulo onde são explicadas as etapas efetuadas na presente investigação que permitem produzir conhecimento científico; Capítulo 3 – Apresentação, Análise e Discussão dos Resultados, capítulo onde é espelhado todo o trabalho de campo efetuado na presente investigação, mais concretamente, são apresentados e analisados os resultados da análise documental, das entrevistas e dos inquéritos; Posteriormente são apresentadas as conclusões, em que são dadas respostas às questões de investigação e tecidas algumas recomendações; Por último, são apresentadas as referências bibliográficas que serviram de apoio e de base para a realização do presente RCFTIA.

CAPÍTULO 1

ENQUADRAMENTO TEÓRICO

1.1. Investigação Criminal na GNR

Ao abordarmos o tema da investigação da GNR para a obtenção de PD, tem-se como referência toda a atividade de IC. Deste modo, antes de abordarmos especificamente as competências e organização da GNR no âmbito da IC, não pode ficar esquecido o conceito que se encontra a montante, ou seja, o próprio conceito de IC.

O conceito de IC vem definido no art. 1º da LOIC (AR, 2008) como “o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo”. A IC tem como objetivo último a recolha de elementos de prova que contribuam para a descoberta da verdade relativamente a factos que constituam crime. Para tal é necessário descobrir de que crime se trata, quais os seus autores, quando ocorreu, onde ocorreu e quais as circunstâncias em que ocorreu o crime (Verdelho, 2004). De forma mais sistemática, a IC procura dar resposta às seguintes questões: “o quê?”, “quem?”, “quando?”, “como?”, “onde?” e “porquê?” (Marques, 2013).

No âmbito do combate à criminalidade, a GNR tem competência para a prevenção e para desenvolver ações de IC que lhe sejam atribuídas por lei ou delegada pela AJ¹. Essa competência é atribuída à GNR através da sua Lei Orgânica² (AR, 2007) e da Lei da Organização da Investigação Criminal (LOIC)³. Neste sentido, como OPC, a GNR “desenvolve um conjunto de acções que visam prevenir a criminalidade em geral e efetuar diligências necessárias tendentes a investigar a existência de um crime e proceder à recolha de prova, determinar os seus agentes, a sua responsabilidade e efectuar as consequentes detenções” (Branco, 2010, p. 246).

Para além de ser um OPC de competência genérica⁴, a GNR tem ainda competência específica para a investigar crimes tributários, fiscais e aduaneiros através da sua unidade especializada – Unidade de Ação Fiscal (UAF)⁵. Neste âmbito, a LOIC estabelece que a

¹ Cfr.: art. 3º n.º 1 als. c), e) e m) da LOGNR.

² Lei n.º 63/2007, de 06 de Novembro.

³ Lei n.º 49/2008, de 27 de Agosto.

⁴ Cfr.: art. 3º n.º 1 al. b) da LOIC.

⁵ Cfr.: art. 3º n.º 1 d) conj. art. 41º n.º 1 da LOGNR.

GNR tem competência para investigar crimes até um valor máximo de €500.000⁶, sendo que a partir desse valor o OPC competente para a investigação é a Polícia Judiciária (PJ).

A atividade de IC na GNR integra um conjunto de técnicas e de procedimentos legalmente admitidos e utilizados de forma sistemática e metódica, orientados para descoberta de factos materiais penalmente relevantes, contribuindo assim para a descoberta da verdade em processo penal (GNR, 2014b).

O modelo da estrutura de IC da GNR está subordinado ao princípio da simplicidade, baseando-se na partilha de tarefas com a estrutura territorial, no que diz respeito à elaboração de inquéritos, em contrapartida também são libertados recursos da estrutura de IC para incremento da atividade operacional (GNR, 2014b).

A estrutura de IC da GNR está concebida por forma a ajustar-se à heterogeneidade e constante mudança dos fenómenos criminais, através de uma distribuição dos meios tendo em conta as áreas com maiores índices criminais. Trata-se de uma estrutura coerente, subordinada a regras de comando e controlo claros, bem como uma coordenação centralizada e de fácil articulação aos diferentes escalões. No que diz respeito à cadeia de comando, esta assenta em relações de dependência técnica, consubstanciando-se assim num canal de comando funcional e extensível a todos os escalões (GNR, 2014b).

Dada a importância desta missão específica, existe no quadro orgânico da GNR a Direção de Investigação Criminal (DIC) como órgão máximo da estrutura de IC e que superintende sob o ponto de vista técnico toda a sua atividade. A principal missão da DIC é coordenar, supervisionar e fazer o registo da atividade da estrutura de IC, através do exercício da autoridade funcional e técnica (GNR, 2014b). A estrutura de IC da GNR vem definida no despacho 18/14, de 21 de Janeiro, bem como as competências dos seus órgãos (GNR, 2014a).

A lógica de funcionamento da estrutura de IC da GNR está centrada nos Comandos Territoriais (CTer), conferindo aos respetivos Comandantes um papel reforçado na condução da atividade de IC, através das respetivas Secções de Informações e Investigação Criminal (SIIC). “Com a centralização das atividades de IC e das informações policiais nas SIIC, não só se reforça a coordenação da rede de Informações da Guarda, como sobretudo se operacionalizam as sinergias entre ambas as capacidades” (GNR, 2014b, p. 2).

É muito importante referir que a IC da GNR é caracterizada pela sua tripla valência: operativa, criminalística e de análise de informação (Branco, 2010). Na vertente operativa

⁶ Cfr.: artº 7º n.º4 al. a) da LOIC.

a GNR é composta por vários tipos de núcleos IC que estão distribuídos pelos CTer sendo que os Núcleos de Investigação Criminal (NIC) e os Núcleos de Investigação de Crimes e Acidentes Rodoviários (NICAV) são os únicos que se encontram, respetivamente, fisicamente sediados nos Destacamentos Territoriais (DTer) e nos Destacamentos de Trânsito, embora dependam funcionalmente das SIIC dos CTer. Os vários núcleos que compõem a vertente operativa são: NIC; Núcleos de Apoio Operativo (NAO); Núcleos de Investigação e de Apoio a Vítimas Específicas (NIAVE); Núcleos de Investigação de Crimes e Contraordenações (NICCO); Núcleos de Investigação de Crimes e Contraordenações Ambientais (NICCOA); e NICAV. A vertente de criminalística é composta por: Núcleos Técnico-Periciais (NTP); e Núcleos de Apoio Técnico (NAT). Por último, a vertente de análise de informação é composta pelos Núcleos de Análise de Informações e Informação Criminal (NAIIC) (GNR, 2014a).

1.2. Prova Penal

Encontrando-se o conceito de prova a montante do conceito de PD é importante defini-lo, caracterizá-lo e enquadrá-lo com a Lei.

Começando com a definição de prova, Mendes (2014) define o conceito de prova segundo duas perspetivas – enquanto atividade probatória e enquanto resultado da atividade probatória. Também Soares (2014) considera importante distinguir o conceito de prova segundo estas duas perspetivas visto que a finalidade da prova é a demonstração da verdade dos factos (Soares, 2014). Assim sendo, enquanto atividade probatória, a prova é “o método através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis” (Mendes, 2014, p. 173). Constituem assim objeto de prova, todos os factos⁷ que se enquadrem com a definição supra referida⁸. Por conseguinte, enquanto resultado da atividade probatória, o autor define o conceito de prova como “a motivação da convicção da entidade decisora acerca da ocorrência dos factos relevantes, contanto que essa motivação se conforme com os elementos adquiridos representativamente no processo e respeite as regras da experiência, as leis científicas e os princípios da lógica” (Mendes, 2014, p. 173).

⁷ Factos jurídicos relevantes para o processo, ou seja, que têm valor na demonstração da existência ou não de um crime, da punibilidade ou não punibilidade do arguido, bem como da determinação da medida da pena ou medida de segurança aplicáveis (Soares, 2015).

⁸ Cfr.: art. 124º n.º1 do Código de Processo Penal (CPP) (AR, 1987).

As provas, enquanto meios de prova, constituem os elementos que podem demonstrar factos relevantes, elementos esses que estão relacionados com a preparação e a prática do crime (Mendes, 2014). Também Soares aborda o conceito de meios de prova e distingue-o dos meios da sua obtenção. No que diz respeito ao conceito de meios de prova, “consistem em todo um conjunto de instrumentos aptos a demonstrar a realidade dos factos relevantes para o processo”⁹ (Soares, 2014, p. 97). Quanto ao conceito de meios de obtenção de prova (MOP) “assumem-se como formas de investigação e de recolha de indícios suscetíveis de comprovar aqueles mesmos factos”¹⁰ (Soares, 2014, p. 97).

Embora os meios de prova obedeçam ao princípio da legalidade¹¹, o CPP tipifica e estabelece o regime para cada um, sendo eles:

- prova testemunhal (art. 128º e ss.);
- declarações do arguido, do assistente e das partes civis (art. 140º e ss.);
- prova por acareação (art. 146º);
- prova por reconhecimento (art. 147º e ss.);
- reconstituição do facto (art. 150º);
- prova pericial (art. 151º e ss.);
- prova documental (art. 164º e ss.).

O objetivo de estar estabelecido o regime que tipifica os meios de prova admissíveis é precisamente garantir a máxima credibilidade dos mesmos para a demonstração dos factos a provar (Mendes, 2014). Em contrapartida ao princípio da legalidade, todas as provas têm de respeitar as regras impostas pelo CPP, no que diz respeito à sua admissibilidade, autenticidade, precisão e integridade (Ramos, 2015). Por conseguinte, apenas a prova obtida nos termos do CPP pode legitimar uma decisão, quer seja ela benéfica (arquivamento do processo¹², decisão instrutória de não pronúncia¹³ ou sentença absolutória¹⁴) ou prejudicial (formulação da acusação¹⁵, decisão instrutória de pronúncia¹⁶ ou sentença condenatória¹⁷) (Soares, 2014).

⁹ O autor dá como exemplo a prova testemunhal e a prova documental.

¹⁰ O autor dá como exemplo as revistas e as buscas.

¹¹ Cfr.: art. 125º do CPP – São admissíveis todas as provas que não forem proibidas por lei.

¹² Cfr.: art. 277º CPP.

¹³ Cfr.: art. 308º CPP.

¹⁴ Cfr.: art. 376º CPP.

¹⁵ Cfr.: art. 283º CPP.

¹⁶ Cfr.: art. 308º CPP.

¹⁷ Cfr.: art. 375º CPP.

A prova¹⁸ é fundamental no processo penal visto que é “com base no exame crítico das provas obtidas que o Tribunal vai fundamentar a sua convicção, condenando ou absolvendo o arguido” (Soares, 2014, p. 95). Refira-se que no sistema português vigora o princípio da imediação¹⁹, ou seja, para que os elementos de prova tenham valor têm obrigatoriamente de ser reproduzidos no decurso do julgamento (Verdelho, 2004).

Da análise dos preceitos processuais relativos à prova, é explícita a preocupação do legislador em conformá-los com os princípios constitucionais, mais concretamente no que diz respeito à dignidade da pessoa humana²⁰, da integridade pessoal²¹ e da intimidade da vida privada e familiar²² (Soares, 2014). Fazendo a ponte entre a preocupação do legislador e os MOP, deve-se ter presente que a par das buscas, as escutas telefónicas são aquelas que são mais suscetíveis de afetar a reserva da intimidade da vida privada das pessoas. É preciso ter presente também que as normas processuais que a Lei do Cibercrime (LC)²³ (AR, 2009) veio implementar assemelham-se muito ao regime das escutas telefónicas, pelo que se pode dizer que as “buscas informático-digitais”²⁴ também são dos MOP mais suscetíveis de afetar a reserva da intimidade da vida privada das pessoas (Ramos, 2015).

Cabe à AJ²⁵ assistida pelos OPC toda a atividade de investigação para a obtenção de prova, embora todos os sujeitos processuais²⁶ possam contribuir para produzir prova e procurar convencer o tribunal da sua versão dos factos. Assim, a GNR, enquanto OPC, e com as respetivas competências de IC delegadas, atua sobre a dependência funcional das AJ, sendo dotada de autonomia técnica e tática de investigação. Embora o MP dirija os inquiridos, não pode dispensar o auxílio dos OPC na tarefa de IC, pois estes são dotados quer de meios técnicos e logísticos, quer de conhecimentos técnicos que são essenciais a esta atividade. Mas, as competências dos OPC não se resume na coadjuvação das AJ, cabendo-lhes também a prática de determinados atos, que por razões de necessidade e urgência, podem partir da iniciativa dos próprios OPC, em especial as medidas cautelares e de polícia²⁷ (MCP) (Soares, 2014).

¹⁸ O CPP regula a matéria relativa à prova no seu Livro III – arts. 124º a 190º.

¹⁹ Cfr.: art. 355º n.º 1 do CPP.

²⁰ Cfr.: art. 1º da Constituição da República Portuguesa (CRP) (AR, 1976).

²¹ arts. 25º e 32º n.º 8 da CRP.

²² Cfr.: arts. 32º n.º 8 e 34º da CRP.

²³ Lei n.º 109/2009, de 15 de Setembro.

²⁴ Expressão utilizada por Armando Dias Ramos.

²⁵ Entenda-se por AJ, o MP (art. 270º n.º 1 e n.º3 do CPP) e o Juiz de Instrução Criminal (JIC) (art. 290º n.º2 do CPP).

²⁶ Para além do Tribunal e do MP, existe o assistente, o arguido, o defensor e as partes civis.

²⁷ Cfr.: art. 248º e sgts. do CPP.

Outro importante assunto relativamente aos meios de prova são os métodos proibidos de prova. “A própria lei estabelece os casos em que as provas não podem ser produzidas, nem valoradas” (Mendes, 2014, p. 175). Uma vez que Portugal se encontra num Estado de Direito Democrático, a realização da justiça e a averiguação da verdade material encontram limites nos supra referidos direitos humanos, constitucionalmente consagrados (Soares, 2014). Neste âmbito, a CRP estabelece no seu art. 32º n.º8 o seguinte: “São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações”.

1.3. Prova digital

1.3.1. Conceito

No âmbito dos inquéritos, os investigadores devem ter presente que podem encontrar muita informação pertinente para anexar aos processos (delegados pela AJ) que esteja contida em dispositivos eletrónicos. Essa informação pode estar contida na internet, em telemóveis, computadores ou qualquer dispositivo que permita o armazenamento de informação sob a forma de bits e bytes. Neste contexto surge o conceito principal de todo este trabalho – o conceito de PD – sendo este “toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações” (Ramos, 2015, pp. 140-141). De uma outra perspetiva, e recorrendo a fontes internacionais, a PD traduz-se em “informação com valor probatório que é armazenada ou transmitida na forma binária” (SWGDE, 2013, p. 7)²⁸.

Da tipificação considerada no subcapítulo anterior referente aos meios de prova, a PD pode ser incluída na prova pericial, “por a mesma exigir especiais conhecimentos técnicos para a sua perceção ou apreciação dos factos” (Ramos, 2015, p. 141). Pode-se ainda classificar a PD como prova documental, sempre que a mesma possa ser corporizada por escrito no processo ou por outro meio técnico, como, por exemplo, a impressão fotográfica ou audiovisual de uma mensagem de correio eletrónico (Ramos, 2015).

A obtenção de PD exige ao investigador não só certos conhecimentos técnicos informáticos, mas também o conhecimento das normas processuais que regem este tipo de

²⁸ Tradução própria.

prova. Um correto manuseamento, transporte, exame e análise de informação contribuem para garantir provas com as características enunciadas no subcapítulo anterior (admissibilidade, autenticidade, precisão e integridade) (Ramos, 2015).

1.3.2. Normas processuais

As normas processuais específicas para a obtenção de PD constam na LC. Esta Lei entrou em vigor em 2009 e “procede à ratificação e implementação da Convenção do Conselho da Europa sobre o Cibercrime, assinada em Budapeste em 23 de Novembro de 2001, e às regras de adaptação interna” (Ramos, 2015, p. 167). Até à data não existiam normas processuais específicas para a obtenção de PD.

Antes das normas processuais propriamente ditas, a LC estabelece, no seu art. 2º algumas definições importantes, entre elas, a de sistema informático, a de fornecedor de serviço, a de interceção e ainda distingue dois tipos de dados: dados informáticos e dados de tráfego. Quanto às normas processuais é importante esclarecer que estas aplicam-se não só a cibercrimes mas também a crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico²⁹.

Relativamente às normas processuais, foram introduzidas a preservação expedita de dados armazenados num sistema informático e a preservação expedita e revelação³⁰ de dados de tráfego (Ramos, 2015). De acordo com o art. 12º da LC, a ordem de preservação desses dados, emitida pela AJ ou por OPC mediante autorização da AJ, deverá ser dirigida a quem tenha a disponibilidade ou controlo desses dados e tem de discriminar certos requisitos, entre eles, o período em que a entidade é obrigada a preservar os dados, que pode ir até um máximo de três meses (sendo que esse período pode ser renovável por períodos também no máximo de três meses, até ao limite máximo de um ano). No que diz respeito à injunção³¹ para a apresentação dos dados é relevante referir que esta não pode ser dirigida ao arguido. “A injunção, no decurso do inquérito, é uma diligência da competência do Ministério Público (MP), que pode ser ordenada sempre que a obtenção dos dados em causa seja necessária à descoberta da verdade” (PGR, 2012, p. 1).

Na investigação de crimes em que são usadas as redes de comunicações, é cada vez mais frequente e necessário obter informação alojada nos fornecedores de serviços de

²⁹ Cfr.: art. 11º n.º 1 da LC.

³⁰ Cfr.: art. 13º da LC.

³¹ Cfr.: art. 14º da LC.

Internet (ISP) estrangeiros (que, por norma, são a estes a quem são dirigidas as injunções suprarreferidas), sendo que a maioria pertence a sociedades com sede nos Estados Unidos da América (EUA). A obtenção dessa informação pode ser feita de duas formas: através de pedidos de cooperação judiciária dirigidos aos EUA, por via da Procuradoria Geral da República (PGR), ou de forma expedita, através do contacto direto entre os magistrados do MP e os ISPs (PGR, 2014a).

Quando a obtenção de informação é feita através da PGR, que atua como autoridade central para fins de cooperação judiciária internacional, o pedido é formulado via carta rogatória, que materializa a formalidade necessária para a obtenção das diligências de inquérito. Contudo, há casos em que essa cooperação não se torna viável, porque as autoridades dos EUA se recusam a prestar as informações pedidas. Tratam-se de casos em que os factos não constituem crime nos EUA, como é o caso da difamação e da injúria, e quando o prejuízo patrimonial seja pouco significativo, pois anualmente são dirigidas milhares de cartas rogatórias às autoridades judiciais dos EUA e assim sendo, estas estabelecem o valor do prejuízo patrimonial como fator para definir prioridades de satisfação. No entanto, quando se trate de criminalidade grave como o terrorismo, crime organizado, corrupção e crime violento, será dada resposta independentemente do valor patrimonial em causa. Existem ainda duas outras situações em que não é viável fazer pedidos de cooperação judicial dirigidos a autoridades dos EUA. A primeira, diz respeito a situações em que já se passaram mais de 90 dias após a prática das comunicações, isto porque os operadores dos EUA guardam os dados de tráfego pelo período de 90 dias e decorrido esse prazo a informação é apagada definitivamente. A segunda, diz respeito às situações em que os pedidos não contenham informação suficiente que permita concluir quais os factos que se investigam ou quais os tipos de crimes envolvidos no inquérito – as autoridades dos EUA exigem que lhes sejam fornecidos os factos investigados no caso concreto, bem como a respetiva qualificação jurídica (PGR, 2014a).

No que diz respeito ao pedido de informações são solicitados diretamente aos ISPs, através do MP, os dados referentes à identificação do titular da conta (nome, morada e endereço IP³² a partir do qual a conta foi aberta), que existem enquanto a conta estiver ativa. Este tipo de informações são bastante úteis para a investigação quando não se obteve previamente prova dos factos ou da identidade do suspeito, podendo ser a única forma de

³² A identificação do endereço IP, que se trata de um número técnico que identifica um dispositivo, estabelece a ligação entre uma determinada comunicação e o respetivo dispositivo que originou a comunicação (Procuradoria Geral da República, 2012).

descobrir quem praticou um determinado crime (PGR, 2015a). Fornecem ainda, quanto aos concretos acessos a contas, a identificação do endereço IP a partir do qual foi feito o acesso (como foi suprarreferido, esta informação é guardada pelo período de 90 dias). O próprio Governo dos EUA “incentiva os prestadores de serviços da Internet a fornecerem às autoridades estrangeiras informações de que disponham, desde que o respetivo pedido seja formulado com respeito pela lei interna do país em causa e pelas leis dos Estados Unidos” (PGR, 2014b).

Para além das medidas processuais aplicáveis à PD suprarreferidas, a LC aborda outras medidas processuais aplicáveis à PD, sendo estas a pesquisa de dados informáticos, a apreensão de dados informáticos, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, a interceção de comunicações e as ações encobertas.

A pesquisa de dados informáticos³³ pode ser autorizada ou ordenada pela AJ quando se torne necessário à produção de prova sendo que, essa autorização tem a validade máxima de 30 dias. A pesquisa pode ainda ser feita pelos OPC sem autorização prévia da AJ em duas situações. A primeira, mediante consentimento do visado, em que esse consentimento fique documentado. A segunda, “nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa”. Nesta última situação o OPC tem a obrigatoriedade de comunicar imediatamente à AJ a diligência efetuada. Em ambas as situações o OPC tem a obrigatoriedade de remeter à AJ competente o relatório em que descreva “as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas”³⁴.

A apreensão de dados informáticos³⁵ pode surgir através de uma pesquisa ou de um acesso legítimo a um dispositivo eletrónico. A LC prevê que os OPC possam apreender PD sem prévia autorização da AJ nos casos em que a pesquisa informática foi legitimamente efetuada ou nos casos em que a demora da apreensão possa por em risco a produção de prova, tratando-se assim de uma MCP. Sempre que seja apreendida PD cujo conteúdo possa pôr em causa a privacidade do respetivo titular ou de terceiro, essa prova tem que ser obrigatoriamente apresentada ao Juiz de Instrução Criminal (JIC), sob pena de nulidade.

³³ Cfr.: art. 15º da LC.

³⁴ Cfr.: art. 253º do CPP.

³⁵ Cfr.: art. 16º da LC.

Quando forem encontradas mensagens de correio eletrónico³⁶, no âmbito da pesquisa ou do acesso legítimo ao sistema informático, o JIC pode autorizar ou ordenar a apreensão das mensagens que possam servir como prova para o processo, sendo que a LC remete para o regime da apreensão de correspondência³⁷ previsto no CPP. Segundo o art. 16º n.º 7 e n.º 8 da LC, a apreensão de PD pode ser feita de três formas (AR, 2009):

- “Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura”;
- “Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; (...) a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital”;
- “Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos”;
- “Eliminação não reversível ou bloqueio do acesso aos dados”.

O recurso à intercepção de comunicações³⁸ é passível de ser realizado nos crimes previstos na LC e nos crimes em que é possível recorrer a escutas telefónicas, sendo que se aplica subsidiariamente o regime das escutas³⁹.

“A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público” (AR, 2009).

Por último, apresenta-se a figura das ações encobertas⁴⁰ que é aplicável aos crimes previstos na LC e também a crimes

“cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no

³⁶ Cfr.: art. 17º da LC.

³⁷ Cfr.: art. 179º do CPP.

³⁸ Cfr.: art. 18º da LC.

³⁹ Cfr. arts. 187º a 190º do CPP.

⁴⁰ Cfr.: art. 19º da LC.

título iv do Código do Direito de Autor e dos Direitos Conexos” (AR, 2009).

No caso de ser necessário o uso de dispositivos informáticos para as ações encobertas aplica-se, na medida do possível, o regime suprarreferido da interceção de comunicações.

1.3.3. Especificações técnicas

Ao longo deste subcapítulo não se pretende fazer aqui uma descrição intensiva dos procedimentos técnicos a adotar nos atos de pesquisa e recolha de PD, até porque ocupariam várias páginas e esses procedimentos encontram-se condensados em guias recolha de PD, sendo que podem ser inclusive consultados, por exemplo, na obra publicada por (Marques, 2013). No que diz respeito aos procedimentos em si, apenas são apresentadas algumas considerações sobre os procedimentos tecidos por Ramos (2015), pois trata-se de uma obra de referência a nível nacional sobre o tema da PD.

Finda a exposição sobre as normas processuais aplicáveis à obtenção de PD torna-se importante expor as etapas a percorrer até chegarmos à obtenção da prova propriamente dita. Marques (2013), apresenta as seguintes etapas:

- 1º Identificação da origem da PD;
- 2º Preservação da prova (pode implicar a duplicação da prova);
- 3º Análise e investigação das provas;
- 4º Apresentação de relatórios ou resultados

Ao ter presente as etapas para a obtenção de prova torna-se mais fácil perceber as críticas doutrinárias no que diz respeito às normas processuais enunciadas. Embora a terminologia apresentada por Marques (2013) não seja precisamente a mesma que é utilizada na LC, as medidas processuais de pesquisa e a apreensão de dados informáticos enquadram-se na segunda etapa.

Ramos (2015) defende que não deve ser confundida a medida de pesquisa de dados informáticos com a pesquisa de dados online. “A primeira, surge no decurso de um processo em investigação, por ser necessário à produção da prova” (Ramos, 2015, p. 148). No que diz respeito à pesquisa de dados online, que é equiparada à intervenção encoberta em sistemas informáticos, existe uma lacuna na lei, pois na opinião do autor,

“o legislador não criou uma norma processual específica para esta novíssima forma de investigação, nem procedeu à sua regulamentação sobre que meios técnicos utilizar, remetendo apenas, no art. 19º da LC,

para o regime aplicável às ações encobertas, previsto na Lei n.º 101/2001, de 25 de agosto. (...) A pesquisa de dados online pressupõe que um sistema informático esteja a ser “vigiado” ou sob interceção, tal qual como se fazem escutas telefónicas, vigilâncias ou seguimentos, como é o caso mais comum em processos de investigação de tráfico de estupefacientes. Uma vez que não se contempla esta figura na lei de modo mais específico, tal como recorrendo a worms ou spyware, a mesma não poderá ser utilizada para desenvolver investigações e carrear prova para um inquérito, sob pena da prova obtida ser considerada nula” (Ramos, 2015, pp. 148-149).

Ramos (2015) aborda também a questão das buscas e apreensões de PD. Segundo o autor, é preciso ter a noção que, quando se realiza uma busca com o intuito de apreender dispositivos informáticos, pode haver muitos cenários com que os elementos policiais se podem deparar, e cada caso tem as suas particularidades. Desde logo, porque não se sabe o que se vai encontrar na busca nem a forma como os visados vão reagir à presença de elementos policiais no seu espaço privado, por outro lado, existem muitos tipos de dispositivos nos quais pode ser guardada informação, o que faz com que a busca seja uma diligência que requer uma atenção reforçada a todos os pormenores (Ramos, 2015). A título de exemplo, Ramos sugere que quando se encontrem dispositivos informáticos desligados no decorrer de uma busca,

“nada mais haverá a fazer se não recolher os mesmos e proceder ao respetivo auto de apreensão, com indicação de todos os elementos que os identifiquem inequivocamente (será assim o caso da marca, modelo, número de série, ou na sua falta a descrição de elementos imutáveis). Defendemos que não deverá proceder-se à ligação do equipamento para efetuar a clonagem do disco, (...) essencialmente, porque o sistema informático guarda em si elementos que poderão ser úteis à investigação, tais como, por exemplo, o último shutdown efetuado, últimos documentos acedidos, etc...” (Ramos, 2015, pp. 149-150).

Outro cenário diferente que Ramos (2015) apresenta é encontrar os dispositivos em plena atividade (ligado ou em modo de hibernação). Um aspeto importante a verificar é se o equipamento está verdadeiramente ligado, porque mesmo estando ligado pode ter um screen saver ativo ou apresentar o ecrã totalmente preto, podendo neste caso, ser observada a luz led (que a generalidade dos dispositivos eletrónicos possui) que indica se o aparelho está ligado. Quando tal suceder, o elemento responsável pela apreensão deve ter presente que um simples clique no rato pode dar início a programas que apaguem informação do dispositivo. Como tal, podem ser executados dois procedimentos:

“mover o rato, sem efectuar nenhum click, ou carregar na barra de espaços do teclado. Com estes procedimentos “acorda-se” o computador e poderá ser possível a visualização dos programas ou aplicações informáticas que estarão a correr naquele momento. Fotografar a imagem

que se encontra no ecrã, após este procedimento, é mais um elemento de prova que poderá ser posteriormente utilizado como prova em tribunal” (Ramos, 2015, p. 151).

Outro importante aspeto a considerar quando se pretenda efetuar a apreensão física dos dispositivos, encontrando-se estes ligados, é a forma de os desligar. À semelhança do que vimos anteriormente, ao desligarmos o dispositivo através dos procedimentos habituais, pode desencadear o início de programas que apaguem informação do disco e inclusive, sem que o elemento policial responsável pela apreensão dê conta. “O método seguro consiste em desligar o equipamento informático diretamente na fonte da energia elétrica e caso estes detenham baterias ou similares deverão ser retiradas, assegurando-se, desta forma, que o terminal informático ficou efetivamente desligado” (Ramos, 2015, pp. 151-152).

Após feita a apreensão física dos dispositivos, segue-se a seguinte etapa na obtenção de prova – o exame forense, definido como “a inspeção sistemática e tecnológica de um sistema informático e dos seus conteúdos, para a obtenção de provas de um crime ou qualquer outro uso que seja investigado” (Marques, 2013).

“O procedimento habitual consiste na realização de uma imagem do suporte físico apreendido (disco rígido, pen USB, ou outro) e é a partir desta imagem (ou clone – sendo esta a expressão mais apropriada) que se vai desenrolar todo o procedimento pericial conducente à elaboração do relatório de exame pericial. Com a vantagem de esta imagem ser realizada com bloqueador de escrita, ou seja, de se preservar toda a informação que existia no suporte original à data da sua apreensão, não havendo qualquer alteração/adulteração de dados” (Ramos, 2015, p. 154).

A PD tem certas especificidades técnicas que fazem dela um tipo de prova delicada, cujo mero descuido a pode tornar inutilizável. “A prova digital conjuga em si vários fatores que a tornam diferente, vulnerável e especial. Por isso, a mesma assume caráter temporário, é fungível e de grande volatilidade” (Ramos, 2015, p. 143).

O caráter temporário prende-se com o facto de haver informação suscetível de desaparecer com o tempo ou que apenas está disponível até um limite temporal definido, exemplo disso é a salvaguarda dos dados de tráfego por parte dos ISP’s, obrigados legalmente a guardar os dados de tráfego pelo período de 1 ano. Ou seja, torna-se uma limitação à investigação por estar limitada a 1 ano a contar do momento da prática do facto para poder produzir prova (Ramos, 2015).

Ramos aborda o caráter fungível bem como o caráter volátil de forma muito simples, referindo que a PD “é fungível porque os dados informáticos facilmente podem ser substituídos por outros. É de grande volatilidade porque poderão ser ocultados ou

suprimidos do suporte original, os quais, sem o uso de uma ferramenta específica, dificilmente serão encontrados” (Ramos, 2015, pp. 144-145).

Outro importante aspeto para a obtenção de PD é o seu transporte, uma vez que os dispositivos eletrónicos são frágeis, e há certos procedimentos a considerar para preservar a informação neles contida. Exemplos de boas práticas será afastar os dispositivos eletrónicos de campos eletromagnéticos (altifalantes, bancos aquecidos, etc.) e transportá-los em sacos anti-estáticos (nomeadamente discos rígidos e placas impressas de circuitos) (Ramos, 2015). A custódia da prova torna-se assim muito importante na obtenção deste tipo de prova, sendo esta se traduz na “documentação cronológica do movimento., localização e posse das provas” (SWGDE, 2013, p. 6)⁴¹.

As boas práticas para a obtenção de PD em Portugal derivam da norma internacional ISO/IEC 27037:2012 "Tecnologias de informação – Técnicas de segurança – Diretrizes para identificação, aquisição, recolha e preservação de prova digital", publicada em 15 de Novembro de 2012. Para além desta norma internacional, também em 2012, o CERT.PT⁴² emitiu uma recomendação que definiu genericamente os cuidados a ter pelas organizações para recolher dados de prova, dando alguns concelhos em função do tipo de crime e referindo algumas ferramentas que poderiam ser utilizadas (Marques, 2013).

O Scientific Working Group on Digital Evidence (SWGDE) identifica três principais categorias de funções para a obtenção de PD (SWGDE, 2004): as equipas de primeira resposta, que incluem equipas responsáveis pela recolha PD no âmbito de buscas e na cena do crime; os examinadores e analistas, que a sua tarefa diária é a recuperação e análise de vestígios digitais; e os técnicos, cuja principal responsabilidade é recolher ou preparar os vestígios digitais para posterior exame e análise.

1.4. Cibercrime e crimes em ambiente digital

O documento que define os Objetivos Estratégicos do MP para 2015-2018, aponta o cibercrime e a PD como área prioritária. Isto deve-se ao facto de haver sido registado um aumento significativo dos crimes contra infraestruturas tecnológicas e também pela necessidade crescente de obter elementos de prova em ambiente digital dos chamados

⁴¹ Tradução própria.

⁴² O CERT.PT trata-se de um serviço do Centro Nacional de Cibersegurança (CNC) que coordena a resposta a incidentes de cibersegurança que envolvam entidades do Estado, operadores de infraestruturas críticas ou outros centros de resposta a incidentes de cibersegurança nacionais (CNCS, s.d.).

“crimes tradicionais”, acompanhando assim o crescimento da utilização da informática no estabelecer das relações profissionais, pessoais e comerciais (PGR, 2015b).

Verdelho identifica três diferentes categorias de fenómenos criminais relacionados com as TIC. Tem-se então os crimes que ocorrem no ambiente informático, mas que podiam ocorrer noutro meio, como é o exemplo das injúrias ou ameaças. Outra categoria apresentada engloba os crimes que ocorrem no meio informático e são típicos dele, ou seja, sem os meios informáticos não é possível cometer esse crime pois estes fazem parte do próprio tipo de crime, como é o exemplo das burlas informáticas. Por último, tem-se a cibercriminalidade propriamente dita, englobando-se nesta categoria os crimes tipificados na LC, compreendidos entre o art. 3º e o art. 8º: falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido (Verdelho, 2015).

CAPÍTULO 2

METODOLOGIA E PROCEDIMENTOS

2.1. Introdução

Existem muitos autores a escrever sobre metodologia científica, cabe ao investigador escolher para o seu trabalho o método que melhor se adapte ao seu objeto de estudo. Desta feita, do ponto de vista da metodologia científica o presente trabalho está enquadrado com os conceitos de Sarmiento e de Marconi & Lakatos.

Neste capítulo pretende-se apresentar a metodologia e os procedimentos efetuados na presente investigação, por forma a explicar o processo de geração de conhecimento científico. Deste modo, entende-se por metodologia científica “*o estudo do método aplicado à ciência*” (Sarmiento, 2013, p. 4). Por conseguinte, o método científico é “um conjunto de procedimentos e de normas que permitem gerar conhecimento” (Sarmiento, 2013, p. 7). Portando, para que um trabalho seja considerado científico tem necessariamente que se apoiar num método que permita gerar conhecimento.

De uma forma mais sintética, a metodologia visa responder às questões “como?”, “com o quê?”, “onde?” e “quanto?”. Por sua vez, estas questões correspondem, respetivamente, ao método de abordagem, aos métodos de procedimento, às técnicas de recolha de dados e à delimitação do universo e da amostra (Marconi & Lakatos, 2003). É assim desta forma que este capítulo se encontra organizado.

2.2. Método de Abordagem e Bases Lógicas

Do ponto de vista do método de abordagem, o presente trabalho segue uma lógica hipotético-dedutiva. Este método básico de investigação, desenvolvido por Karl Popper, “baseia-se na formulação de hipóteses ou conjeturas, que melhor relacionam e explicam os fenómenos” (Sarmiento, 2013, p. 9). Marconi & Lakatos (2003) explica este método por etapas, em que o ponto de partida é a criação de um problema, dizendo respeito à formulação das questões de investigação. A esse problema é proposta uma solução provisória, denominada de “hipóteses”, e que neste caso dizem respeito às perceções do investigador face ao estudo exploratório que foi feito, com base na leitura de artigos e da aplicação de entrevistas exploratórias a oficiais da GNR. Posteriormente, a recolha e

análise de dados vão gerar conhecimento para, na fase final, submeter as hipóteses inicialmente formuladas aos testes de falseamento. Assim, as hipóteses “são testadas, de modo a confirmar quais são as válidas, ou seja, aquelas em que não há razões para refutar as hipóteses” (Sarmiento, 2013, p. 9). No que diz respeito às questões de investigação e hipóteses, estas podem ser consultadas na introdução do presente RCFTIA.

Ao nível dos procedimentos de investigação foram cumulativamente aplicados os métodos demonstrativo e inquisitivo. O método demonstrativo “apoia-se na execução de uma dada operação, destacando-se as técnicas, as ferramentas e os materiais mais adequados para explicar o que se pretende” (Sarmiento, 2013, p. 7). O método inquisitivo “é baseado no interrogatório escrito ou oral” (Sarmiento, 2013, p. 8). Como se pode ver mais à frente, quando falarmos das técnicas de recolha de dados, a nossa análise documental enquadra-se no conceito do método demonstrativo enquanto que as entrevistas e questionários aplicados se enquadram no conceito de método inquisitivo.

2.3. Métodos e Técnicas de Recolha de Dados

“Para que a informação recolhida no universo informacional seja fiável e os resultados da investigação sejam válidos, os instrumentos e métodos científicos utilizados, devem ser apropriados” (Sarmiento, 2013, p. 27). Assim sendo, de acordo com os tipos de instrumentos apresentados por Sarmiento (2013), a recolha de dados efetuada no presente trabalho está apoiada em: análise documental, em entrevistas e em inquéritos.

Quanto aos instrumentos utilizados, pode-se classificar a presente investigação como sendo mista, uma vez que utiliza informação quantitativa, mais concretamente fornecida pela análise documental e através das entrevistas e dos questionários, obtém-se informação qualitativa (Sarmiento, 2013).

2.3.1. Análise Documental

“A análise documental é produzida pelo investigador relativamente a fontes primárias, fontes secundárias e fontes bibliográficas que podem ser contemporâneas ou retrospectivas” (Sarmiento, 2013, p. 27).

Foi solicitado ao CTer de Coimbra a cedência do registo de dados relativo aos exames forenses (no âmbito da PD) elaborados pelo seu NTP em 2015. Este registo de dados contém, essencialmente, informações quanto a:

- Tipos de dispositivos eletrónicos examinados;
- Número Único de Identificador de Processo Crime (NUIPC);
- Data da realização do exame;
- Órgão responsável pelo inquérito;
- Tipo de crime a investigar no inquérito – de acordo com a tipificação feita no mapa para notação de crimes – Modelo 262.

Este registo de dados tem um peso muito importante para a presente investigação pois a sua análise foi o ponto de partida de todo o trabalho de campo. Segundo Sarmiento (2013), esta é uma fonte de informação secundária do tipo dois, visto ser produzida por terceiros e ser uma estatística de uma instituição.

Foi também feita uma análise ao Relatório Anual de Segurança Interna (RASI) de 2015 (SSI, 2015), referente ao número de exames e perícias no âmbito das tecnologias de informação e comunicação. Segundo Sarmiento (2013), esta é uma fonte de informação secundária do tipo um, visto que é produzida por terceiros e é uma estatística feita ao nível nacional.

2.3.2. Entrevistas

A entrevista trata-se de um tipo de instrumento que “permite explorar um domínio e aprofundar o seu conhecimento através da inquirição presencial a um ou mais indivíduos. Os seus conteúdos são mais ricos em informação” (Sarmiento, 2013, p. 28). Basicamente, uma entrevista é “um conjunto de perguntas (designado por guião), que são respondidas necessariamente por via oral” (Sarmiento, 2013, p. 30).

Foram realizadas entrevistas com o intuito de determinar a importância da PD para a GNR. Do ponto de vista do investigador, a IC é um trabalho conjunto entre o MP e o OPC, em que o primeiro dirige o inquérito e delega os atos de investigação, ou parte deles, nos segundos, sendo estes dotados de autonomia técnica e tática para cumprir os objetivos propostos pelo MP. Atendendo ao exposto, decidiu-se aplicar entrevistas quer a Magistrados do MP quer a Oficiais da GNR da estrutura de IC, de modo a obter contributos dos dois pontos de vista.

Foi ainda aplicada uma entrevista isolada a um elemento do NTP do CTer de Coimbra, tendo em vista obter resposta a uma das QD. Embora pudesse ser dada resposta a esta questão de investigação recorrendo a outro instrumento, como a observação direta, do ponto de vista do investigador constatou-se ter uma validade reforçada se questionarmos diretamente um especialista e ficarmos com o registo escrito do seu discurso.

Quanto à preparação das entrevistas, foram seguidos os princípios definidos por Marconi & Lakatos (2003) em que, na construção da entrevista foi elaborado um guião inicial, revisto e alterado por dois especialistas, nomeadamente o Orientador e Coorientador da presente investigação. Os guiões finais podem ser consultados nos Apêndices A e B.

No que diz respeito à classificação apresentada por Sarmiento (2013), as entrevistas aplicadas no presente trabalho classificam-se como:

- presenciais, quanto ao modo;
- exploratórias, quanto ao tipo;
- individuais, quanto ao número de pessoas;
- semiestruturadas, quanto à estruturação.

2.3.2.1. Caracterização da Amostra

“O universo ou população é o conjunto de indivíduos (...) com uma ou mais características comuns, que se pretende analisar ou inferir” (Sarmiento, 2013, p. 71). Segundo esta definição, no âmbito das entrevistas aplicadas, a presente investigação tem dois universos distintos:

- O universo dos magistrados do MP e dos Oficiais da estrutura de IC da GNR;
- O universo dos militares da componente criminalística da GNR que realizam os exames forenses para obtenção de PD (NTP Coimbra).

A amostra é um “conjunto de elementos retirados da população, que é representativo e significativo desta população” (Sarmiento, 2013, p. 71). Quanto à amostra referente ao primeiro universo suprarreferido, foram selecionados, com base em entrevistas exploratórias, alguns dos Magistrados do MP e os Oficiais da GNR que têm um conhecimento mais amplo do tema a nível nacional. Apresenta-se sinteticamente a amostra na tabela 1, sendo a tabela também nos fornece informações quanto ao espaço e tempo em que cada entrevista foi efetuada.

Tabela 1: Caracterização dos Entrevistados.

Entrevistados		Função	Data	Local
E1	Dr. Pedro Verdelho	Coordenador do Gabinete de Cibercrime da PGR	10-05-2016	Lisboa
E2	Dr. Rui Cardoso	Coordenador do DIAP de Sintra	12-05-2016	Sintra
E3	Dr. Carlos Pinho	Procurador Adjunto do DIAP de Aveiro	13-05-2016	Aveiro
E4	Coronel Vivas	Chefe da Divisão de Criminalística da GNR	13-05-2016	Alcabideche
E5	Major Botas	Cmdt da SIIC do CTer de Lisboa	16-05-2016	Lisboa
E6	Major Machado	Adjunto do Cmdt da SIIC do CTer Coimbra	16-05-2016	Coimbra

Fonte: Elaboração própria.

Uma vez que a amostra contempla magistrados do MP e oficiais da GNR com diferentes funções, conseguiu-se obter contributos de vários pontos de vista permitindo, por sua vez, enriquecer as conclusões, mantendo a IC como denominador comum da amostra. Apesar de nem todos os elementos possuírem informação atualizada para responder concretamente a todas as questões formuladas, trata-se de um guião composto por perguntas de grande relevância para o objeto de estudo, no qual todas as respostas obtidas se mostraram pertinentes.

Quanto à amostra dos militares do NTP de Coimbra, foi entrevistado o Sr. Cabo Rodrigues. Uma vez que o núcleo é constituído por 3 militares (universo), considerámos ser necessário aplicar a entrevista apenas a um dos seus constituintes, sendo que o critério de escolha foi baseado na hierarquia, tem sido escolhido o militar com a patente mais alta. Essa entrevista foi realizada em Coimbra no dia 16-05-2016.

Tendo por base os conceitos de Sarmiento (2013) sobre o processo de amostragem, verifica-se estar perante um tipo de amostra não probabilística e intencional, uma vez que foram selecionados elementos que, com base nas opiniões de várias pessoas que conhecem as características específicas do objeto de estudo, são mais representativos da população.

2.3.3. Inquéritos por Questionário

O Inquérito “é um conjunto de perguntas (designado por questionário), que são respondidas obrigatoriamente por escrito” (Sarmiento, 2013, p. 30). Este instrumento de investigação “permite conhecer e aprofundar o conhecimento através das opiniões de vários indivíduos, de uma forma incisiva (Sarmiento, 2013, p. 28).

Quanto ao processo de elaboração dos inquéritos por questionário, foram seguidos os princípios definidos por Marconi & Lakatos (2003). Assim sendo, à semelhança do procedimento suprarreferido para as entrevistas, depois de elaborado, o questionário foi revisto e alterado pelo Orientador e pelo Coorientador da presente investigação. Após esta validação, o questionário foi aplicado presencialmente a dois chefes do CTer Lisboa, para que pudessem ser detetados alguns erros ou problemas de interpretação das questões, cumprindo-se assim a fase do pré-teste.

Os questionários foram divulgados por todos os chefes de núcleos IC da GNR, da componente operativa, com o objetivo de recolher contributos sobre a importância da PD e também sobre as capacidades e dificuldades dos investigadores para a obtenção de PD. O questionário, que pode ser consultado no Apêndice C, divide-se em três grandes partes. Na primeira, é feita uma apresentação e explicação dos objetivos. A segunda parte contempla um conjunto de perguntas respeitantes à caracterização sociodemográfica dos inquiridos. Na terceira parte, são então feitas as questões de conteúdo, correspondendo a um total de dezoito questões fechadas, com base na escala de Likert, composta por cinco níveis (Sarmiento, 2013). Os questionários foram difundidos e respondidos através de um servidor online denominado *SurveyMonkey* e respondidos entre 09-05-2016 e 17-05-2016. A análise aos mesmos foi efetuada com recurso ao programa informático *Microsoft Excell*.

2.3.3.1. Caracterização da Amostra

No âmbito dos inquéritos por questionário, o universo corresponde a todos os chefes dos núcleos IC, da componente operativa, dos CTer a nível nacional. Os núcleos IC são constituídos por 86 NIC, 24 NIAVE, 20 NICAV, 17 NAO, 4 NICCO e 18 NICCOA. A amostra corresponde a 46 NIC, 15 NIAVE, 9 NICAV, 9 NAO, 4 NICCO e 5 NICCOA, perfazendo um total de 88 inquéritos respondidos.

No que diz respeito à caracterização sociodemográfica da amostra, no total dos 88 inquiridos apresentam-se os seguintes dados:

- Uma média de 41,5 anos de idade;
- 79 elementos do sexo masculino e 9 do sexo feminino;
- Quanto ao grau de escolaridade, 18 com o 11º ano ou inferior, 59 com o 12º ano, 8 com licenciatura, 1 com mestrado, 1 com pós-graduação e 1 com doutoramento;
- Quanto ao posto, 1 Guarda Principal, 17 Cabos, 4 Cabos Chefe, 2 Cabos Mor, 8 Segundos Sargento, 31 Primeiros Sargento, 24 Sargentos Ajudante e 1 Sargento Chefe.
- Uma média de 9,7 anos de experiência na estrutura de IC.

CAPÍTULO 3

APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

3.1. Introdução

No presente capítulo, apresentam-se e analisam-se todos os dados coletados relativamente ao trabalho de campo. Neste âmbito, começa-se por apresentar a análise de conteúdo, relativamente aos exames forenses efetuados pelo NTP de Coimbra, em 2015. De seguida, apresenta-se a análise das entrevistas efetuadas a magistrados do MP, a oficiais da GNR da estrutura de IC e também a um elemento do NTP de Coimbra. Para finalizar a análise dos resultados, apresentam-se os dados relativos aos inquéritos por questionário aplicados aos chefes dos núcleos IC, dos CTer.

3.2. Análise Documental

Como referido no ponto 2.4.1., foi efetuada uma análise ao conteúdo do registo de dados relativo aos exames forenses exportados pelo NTP do CTer de Coimbra, em 2015, constituindo-se o único órgão da GNR a realizar este tipo de exames. Por forma a enquadrar o número de exames forenses efetuados, apresentam-se, nas tabelas 2 e 3, a estatística relativamente a todos os exames efetuados a nível nacional, particularizando também os que foram efetuados pela GNR.

Tabela 2: Exames e perícias no âmbito das tecnologias de informação e comunicação.

Unidades	Ano 2015
Pedidos	6.460
Realizados	8.186

Fonte: Adaptado de RASI 2015 (SSI, 2015).

Tabela 3: Exames forenses no âmbito das tecnologias de informação e comunicação, efetuados pela GNR.

Unidades	Ano 2015
Pedidos	744
Realizados	940

Fonte: Adaptado de NTP Coimbra.

Como se pode constatar, a GNR contribuiu com 11,5% dos exames forenses realizados a nível nacional. Nos 940 exames forenses realizados pela GNR estão

envolvidos 144 processos judiciais. Salienta-se que o número de exames realizados é superior ao número de exames pedidos porque, por vezes, ao mesmo dispositivo eletrónico pode ser necessário fazer vários exames, em virtude de haver várias componentes desse dispositivo que possam conter informação, como por exemplo, o exame a um telemóvel pode implicar não só o exame à sua memória interna, mas também a outras componentes nele contidas como o cartão SIM ou cartão de memória.

A tabela 3 revela os tipos de TIC sujeitas a exame forense. É importante referir que o registo de dados utilizado como fonte deste trabalho está organizada por exame forense, mas, tendo em conta que não foi possível determinar com precisão quantos dispositivos eletrónicos estão envolvidos em cada inquérito, foi delimitado o objeto de estudo em função dos inquéritos judiciais e incidiu-se a análise na determinação das TIC examinadas em cada inquérito. Importa também esclarecer que há inquéritos nos quais foram efetuados exames a mais do que um tipo de dispositivo.

Tabela 3: Tipos de TIC examinados nos inquéritos judiciais.

Equipamentos/ tipos de exame	N.º de inquéritos
Telemóveis	123
Computadores	23
Dispositivos de armazenamento	12
Tablets	11
GPS	6
Máquinas fotográficas digitais	4
Análise de registos de comunicações (operadoras)	3
Extração de dados contas online	3
Extração de metadados de correio eletrónico	2
Cameras de filmar	1
CD/DVD	1
Modem Router	1
Total	144

Fonte: Adaptado de NTP Coimbra.

Entre os 940 exames realizados identificam-se 12 categorias de TIC, como pode ser visto na tabela 3, na qual a grande maioria são exames a dispositivos eletrónicos, mas também verificam-se algumas categorias que não envolvem a pesquisa direta nos dispositivos, como é, por exemplo, o caso da análise de registos de comunicações. Como se pode comprovar, a categoria dos telemóveis, onde se incluem também os smartphones e os componentes que possam estar neles contidos (como os cartões SIM e cartões de memória), é o tipo de dispositivo examinado na grande maioria dos inquéritos, para obtenção de PD, perfazendo um total de 123 inquéritos. Embora não esteja espelhado na

tabela, em função do número de exames realizados, a proporção de telemóveis e os seus componentes examinados também não se encontrará muito longe da proporção que é espelhada em função no número de inquéritos. Como segunda e terceira maiores categorias de equipamentos examinados apresentam-se, respetivamente, os computadores, onde se incluem os computadores de secretária, computadores portáteis, etc., em 23 inquéritos e os dispositivos de armazenamento, onde se incluem os discos externos, dispositivos pen drive e cartões de memória, em 12 inquéritos. As categorias que se revelam de menor relevo são os modems router, os CDs e DVDs e as cameras de filmar, em apenas 1 inquérito, cada uma destas categorias.

Outro importante nível de análise do registo de dados foi quanto ao tipo de crime associado aos inquéritos que deram origem aos exames forenses. No total dos 144 inquéritos judiciais que deram origem aos exames forenses, identificam-se 25 tipos de crime, como pode ser observado na tabela 4⁴³.

Tabela 4: Tipos de crime investigados nos inquéritos judiciais.

Tipos de crime	N.º de inquéritos
Tráfico de estupefacientes	50
Violência doméstica contra cônjuge ou análogos	26
Contra os direitos de autor	18
Burla informática e nas comunicações	7
Ameaça e coação	7
Outros furtos	4
Difamação, calúnia e injúria	4
Furto em estabelecimento de ensino com arrombamento, escalamento ou chaves falsas	4
Lenocínio e pornografia de menores	3
Ofensa à integridade física voluntária grave	2
Furto de veículo motorizado	2
Outros crimes	2
Devassa da vida privada e violação de segredo	2
Furto em residência com arrombamento, escalamento ou chaves falsas	2
Outros roubos	1
Recetação e auxílio material	1
Burla relativa a seguros	1
Desobediência	1
Furto em edifício comercial ou industrial com arrombamento, escalamento ou chaves falsas	1
Extorsão	1
Tráfico de pessoas	1
Violação de domicílio e introdução em lugar vedado ao público	1
Furto de metais não preciosos	1
Maus tratos a animais de companhia	1
Furto em outros edifícios com arrombamento, escalamento ou chaves falsas	1
Total	144

Fonte: Adaptado de NTP Coimbra.

⁴³ Pode ser consultado no Apêndice D, o gráfico correspondente à tabela 4

Os três tipos de crime com maior expressão são: tráfico de estupefacientes, punido pela Lei n.º 15/93, de 22 de Janeiro (AR, 1993), em 34,7% dos inquéritos; crime de violência doméstica contra cônjuge ou análogos, punido pelo art. 152º do CP (AR, 1995), em 18,1% dos inquéritos; e o crime contra os direitos de autor, punido pelo DL n.º 63/85, de 14 de março (AR, 1985), em 12,5% dos inquéritos. Os crimes contra o património também assumem aqui uma grande relevância, embora cada tipo de crime por si não tenha uma grande expressão. Estão envolvidos um total de 26 crimes contra o património, correspondendo a cerca de 18.1% dos inquéritos. Entre os crimes contra o património, por ordem de relevância, tem-se: burla informática e nas comunicações; outros furtos; furto em estabelecimento de ensino com arrombamento, escalamento ou chaves falsas; furto de veículo motorizado; furto em residência com arrombamento, escalamento ou chaves falsas; outros roubos; extorsão; furto de metais não preciosos; recetação e auxílio material; burla relativa a seguros; furto em edifício comercial ou industrial com arrombamento, escalamento ou chaves falsas; e furto em outros edifícios com arrombamento, escalamento ou chaves falsas. Todos estes crimes contra o património são punidos pelo CP (AR, 1995).

Através do NUIPC, consegue-se saber qual o OPC ou judicial responsável pelo registo da notícia de crime, relativamente aos processos que deram origem aos exames forenses.

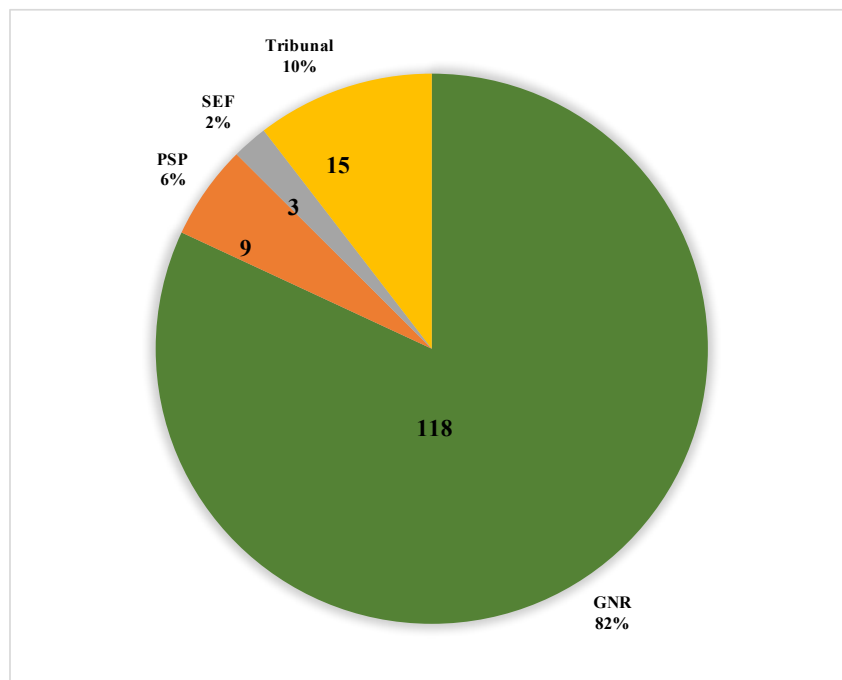


Figura 1: Percentagem de inquéritos com dispositivos eletrónicos no NTP da GNR por órgão policial ou judicial que registou a notícia de crime.

Fonte: Adaptado de NTP Coimbra.

Como se pode constatar na figura 1, a grande maioria dos processos (118) teve origem na GNR. Na nossa opinião, o facto de os exames terem sido realizados num órgão da GNR tem influência nos resultados, mas estes números devem-se também porque, entre os órgãos apresentados, a GNR é o órgão que apresenta uma maior dispersão territorial, tendo à sua responsabilidade cerca de 94% do território nacional e, como tal, é normal que receba um maior número de registos de notícia de crime.

De outro ponto de vista, foi possível analisar a origem dos inquéritos em que houve a intervenção do NTP Coimbra, por unidades da GNR e Serviço de estrangeiros e fronteiras (SEF). Esta análise dá-nos um panorama a nível territorial dos pedidos que são feitos para a realização dos exames forenses. Como se pode ver na figura 2, com base nesta análise de conteúdo, conseguiu-se saber quais as unidades da GNR/serviços exteriores à GNR e também o número de inquéritos que deram origem aos exames forenses para obtenção de PD.

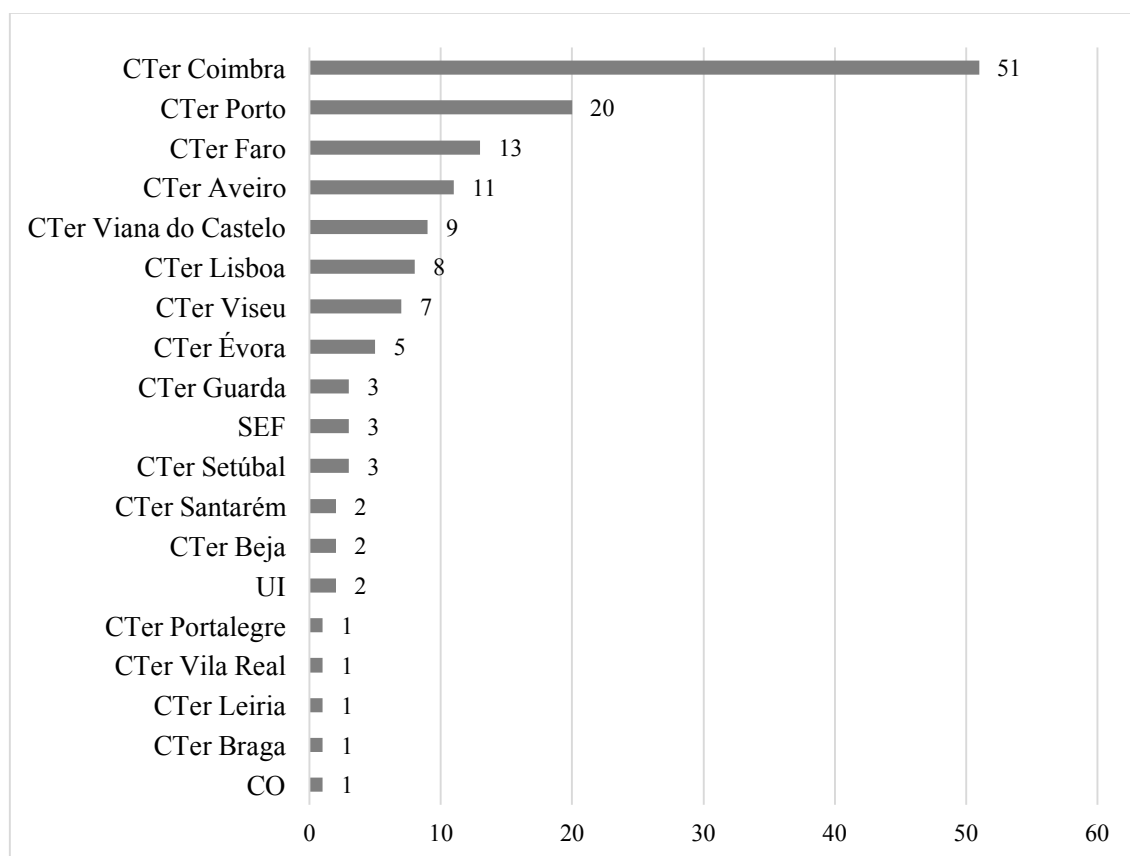


Figura 2: Quantidade de inquéritos crime por Unidade da GNR e SEF que necessitaram de recolher prova por via de exames forenses realizados no NTP da GNR.

Fonte: Adaptado de NTP Coimbra.

Da análise da figura 2 conclui-se que os CTer que, no ano de 2015, mais contribuíram para a obtenção de PD através de exame forense, e socorrendo-se desta valência da GNR são: Coimbra, com 35,4% dos inquéritos; Porto, com 13,9%; e Aveiro com 7,6%. Uma vez que o NTP com esta valência está sediado em Coimbra, entende-se ser normal este CTer a fazer mais pedidos de exame, pois, para além de terem um contacto mais direto e próximo, permite-lhes ter um conhecimento melhor das capacidades do NTP. Em contrapartida, alguns CTer não têm registos de inquéritos em que houvesse pedidos de exames ao NTP de Coimbra, como são os casos de: Bragança; Castelo Branco; Açores; e Madeira. Pode-se constatar também que para além do dispositivo territorial, existem outras unidades da GNR que contribuíram com pedidos de exames forenses para obtenção de PD, como foi o caso da Unidade de Intervenção (UI) e do Comando Operacional (CO). Verifica-se também que, embora seja um número pouco significativo (3 inquéritos), existe cooperação entre a GNR e o SEF nesta área. Apresenta-se, no Apêndice E, o gráfico que espelha quais os órgãos da GNR que estão na origem dos pedidos de exame forense e o respetivo número. Entre estes, a grande maioria pertence à estrutura dos CTer: NAO, NAT, NIAVE, NIC, NICCOA e as Secções de Inquéritos dos Postos Territoriais (PTer). Registam-se também pedidos efetuados pela Secção de Investigação Criminal (SIC) do Grupo de Intervenção de Operações Especiais e pela DIC, inseridos na figura 2 como UI e CO. Os serviços exteriores à GNR são revelados na tabela como não determinados (n/d) e dizem respeito àqueles que foram pedidos diretamente pelo tribunal ou pelo SEF.

3.3. Análise das Entrevistas

O presente subcapítulo visa apresentar e analisar os resultados obtidos nas entrevistas. Para a apresentação dos resultados utilizaram-se tabelas que sintetizam as ideias principais retiradas das respostas (os segmentos) e as respetivas percentagens. A lista de segmentos é apresentada no Apêndice F enquanto que o quadro de análise de conteúdo das entrevistas se encontra no Apêndice G.

3.3.1 Análise de Conteúdo à Questão 1

A tabela 5 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 1: “Considera ser relevante que a IC priorize a PD para os inquéritos?”

Como primeira grande conclusão a retirar, de facto, a PD é um tipo de prova que pode ser obtida no âmbito de vários crimes e, como tal, deve ser priorizada para os inquiridos. Todos os entrevistados o constataram e também é unânime que a criminalidade cometida através das TIC tem vindo a aumentar, sendo que a tendência é para aumentar ainda mais. Engloba-se aqui também os crimes tradicionais que, mesmo não cometidos tipicamente através dos sistemas de informação, possam ter PD envolvida (Verdelho, A importância da Prova Digital, 2016). Com base nos contributos obtidos nas entrevistas, realça-se que, embora a cibercriminalidade propriamente dita, da competência reservada da PJ, esteja a aumentar, a criminalidade com mais expressão é a “tradicional”, da competência genérica de investigação da GNR (no âmbito da PD).

São também apontadas duas razões essenciais para explicar o aumento deste tipo de criminalidade. A primeira é que os sistemas de informação são acessíveis a grande parte da população. A outra razão apontada prende-se com o facto de que, para além dos sistemas de informação serem de fácil acesso, é bastante simples para o comum cidadão operá-los, não sendo necessária formação específica (Pinho, 2016).

Tabela 5: Análise Qualitativa e Quantitativa das Respostas à Questão n.º1.

Segmentos das Respostas	Entrevistados						Frequência (n)	Percentagem (%)
	1	2	3	4	5	6		
Questão n.º1: Considera ser relevante que a IC priorize a PD para os inquiridos?								
Segmento 1a	X	X	X	X	X	X	6	100%
Segmento 1b	X	X	X	X	X	X	6	100%
Segmento 1c	X	X	X		X	X	5	83,3%

Fonte: Elaboração própria.

3.3.2. Análise de Conteúdo à Questão 2

A tabela 6 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 2: “Considera que as capacidades técnicas dos investigadores da GNR e as rotinas processuais são adequadas para a obtenção de prova digital?”.

A maior parte dos entrevistados (83,3%) são da opinião de que as capacidades técnicas dos investigadores da GNR não se encontram ajustadas à obtenção de PD. Também são referidos alguns exemplos nas entrevistas, em especial, no decorrer de buscas efetuadas pelos investigadores da componente operativa da GNR, referindo não estarem

capacitados para fazer pesquisas nos computadores sem alterar nada nos mesmos. Também é reconhecido que isto não se aplica em todo o dispositivo e é apontado um exemplo de sucesso onde já se evoluiu nesse sentido, como é o caso do CTer de Coimbra (Cardoso, 2016). Por outro lado, 83,3% dos entrevistados também são da opinião que a GNR já está a fazer um esforço e a criar estruturas para fazer face a esta realidade. Exemplo disso foi a criação da Repartição de Análise Forense Digital (RAFD), nas instalações da DIC, que iniciou atividade em 2016 (Vivas, 2016). Deste modo, a GNR ficou capacitada para realizar exames forenses para recolha de PD em Coimbra e Alcabideche, sendo que em Coimbra esta capacidade já se encontrava em funcionamento.

Ao nível da formação, 33,3% dos entrevistados consideram que o tema da PD deve ser do conhecimento, no mínimo, do efetivo com funções na estrutura da IC. Ainda assim, apontam como objetivo ideal ter todo o efetivo da GNR com conhecimentos nesta área, como tal, deve ser integrado na formação inicial, não dispensando a formação contínua, pois trata-se de um tema muito evolutivo. Isto deve-se essencialmente porque quem recebe grande parte das denúncias e a quem as pessoas se dirigem muitas vezes para esclarecer dúvidas é precisamente aos militares do efetivo territorial, assumindo-se assim importante que estes saibam atuar nestas situações. Neste âmbito, Pinho (2016) refere, a título de exemplo, que o militar deve saber explicar a uma pessoa como se recolhe o cabeçalho técnico de uma mensagem de correio eletrónico, assim como também deve o próprio militar saber redigir o auto de notícia com as particularidades próprias, relativas à PD. Contudo, 33,3% dos entrevistados, referem haver CTer onde já existe esta preocupação e onde é dada formação específica no âmbito da PD.

É referido por 33,3% dos entrevistados que a implementação de procedimentos seria uma boa forma de colmatar algumas lacunas. Como refere Pinho (2016), em Aveiro já existe um guia prático para recolha de PD e os militares da GNR desse CTer já o aplicam. A existência de um manual condensa conhecimentos técnicos e legais que são aplicados à recolha de PD, ou seja, a criação de um manual deste tipo aplicável a todo o dispositivo permite aos militares ter um suporte de apoio sempre que hajam dúvidas. Associado a isto, 16,7% dos entrevistados refere explicitamente ser importante ter os conhecimentos técnicos e legais aplicáveis à recolha de PD.

Verdelho (2016) é da opinião de que não é função dos investigadores, muito menos dos militares do efetivo territorial, saber extrair PD de um dispositivo eletrónico. Isto vai muito ao encontro também da opinião de Pinho (2016), referindo este último na entrevista

um modelo aplicado a grande parte das polícias de todo o mundo. Este modelo, definido pela International Organization for Criminal Digital Evidence (IOCE), estipula três níveis de obtenção de PD. O primeiro nível, designado de “nível de primeira resposta”, é o nível básico de obtenção de PD. Para este nível basta alguma formação básica (cerca de 2 dias de formação), equipamento adequado e consiste na recolha de dados informáticos em sistemas informáticos simples, como é o caso dos comuns smartphones. Pinho (2016) refere ser um passo fundamental e obrigatório para as polícias portuguesas avançarem no sentido de, em cada Comando Distrital, haver equipas próprias e capacitadas para fazer este tipo de recolha de prova em tempo útil. Quanto ao 2.º nível de recolha de PD, é o nível de “exame forense”, este sim tem de ser feito por especialistas, pois tem um nível de complexidade mais elevado. A este nível, como já foi referido, neste momento a GNR tem o NTP de Coimbra e a RAJD de Alcabideche.

Por último, 33,3% dos entrevistados dão grande ênfase à urgência na obtenção de PD, sendo que esta deve ser acautelada logo desde o momento da notícia do crime, ou seja, logo quando é feita a denúncia, ou, caso não seja possível, deve ser obtida antes do primeiro interrogatório judicial. Articulado com os conceitos que suprarreferidos, as equipas do nível de primeira resposta servem para dar apoio mais próximo e em tempo útil atuando precisamente neste âmbito.

Tabela 6: Análise Qualitativa e Quantitativa das Respostas à Questão n.º 2.

Segmentos das Respostas	Entrevistados						Frequência (n)	Percentagem (%)
	1	2	3	4	5	6		
Questão n.º1: Considera que as capacidades técnicas dos investigadores da GNR e as rotinas processuais são adequadas para a obtenção de PD?								
Segmento 2a	X	X	X	X	X		5	83,3%
Segmento 2b	X	X		X	X	X	5	83,3%
Segmento 2c	X		X				2	33,3%
Segmento 2d	X		X				2	33,3%
Segmento 2e			X				1	16,7%
Segmento 2f			X		X		2	33,3%
Segmento 2g	X						1	16,7%
Segmento 2h	X	X					2	33,3%

Fonte: Elaboração própria.

3.3.3. Análise de Conteúdo à Questão 3

A tabela 7 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 3: “Considera que a GNR tem contribuído de forma eficaz para que as provas obtidas (âmbito da PD) na investigação sejam validadas?”. Uma vez que nem todos os entrevistados responderam a esta questão, as percentagens também se relevam mais baixas.

Contudo, grande parte das respostas apontam no sentido da GNR ainda ter muita margem de progressão para contribuir de forma mais eficaz para a validação das provas. Pinho (2016) apresenta uma opinião bastante consolidada, defendendo que a GNR ainda não contribui de forma eficaz para a validação das provas. São apontadas 3 razões essenciais para que isso aconteça: em primeiro lugar, ainda há a tendência para passar a PD a prova documental, o que desvirtua o teor da prova; em segundo, a preservação das provas ainda não está a ser feita do modo ideal, uma vez que o comum militar ainda não tem os conhecimentos para o fazer nem para explicar, por exemplo a um cidadão que apresente uma queixa crime por ameaça através dos sistemas de informação, como é que o próprio cidadão pode fazer essa preservação da prova; por último, a GNR ainda não está capacitada com equipas de primeira resposta com conhecimentos técnicos e equipamentos apropriados para fazer essa recolha de PD. Com 33,3%, constata-se que a GNR ainda não se encontra vocacionada para a obtenção de PD, pois ainda apoia-se muito noutros tipos de prova. É referido, neste âmbito que, hoje em dia, os investigadores apoiam-se muito num modelo de investigação que baseada em vigilâncias e escutas telefónicas, pelo que este modelo já não é adequado a todos os tipos de crime e vê-se, portanto, uma necessidade de inovar (Botas, 2016).

Constata-se também que a vertente criminalística da GNR se encontra mais desenvolvida, cumprindo as melhores práticas internacionais e atuando em conformidade com a lei processual penal aplicada à PD. Os investigadores do CTer Coimbra também já contribuem de forma eficaz uma vez que a Unidade tem dado formação sobre o tema, e não menos importante é o contato próximo que têm com o NTP, permitindo esclarecimentos das questões mais técnicas em tempo útil (Machado, 2016).

Um pouco de encontro àquilo que foi referido na questão n.º 2, 33,3% dos entrevistados abordam a questão das MCP e do conhecimento das normas penais aplicadas a este tipo de prova que se encontram na LC e no CPP. Vivas (2016) assegura que a atividade criminalística da GNR cumpre todo o normativo em vigor a para além disso

aplica em todos os processos as melhores práticas internacionais, emanadas pela International Association of Computer Investigative Specialists (IACSIS).

Tabela 7: Análise Qualitativa e Quantitativa das Respostas à Questão n.º3.

Segmentos das Respostas	Entrevistados						Frequência (n)	Porcentagem (%)
	1	2	3	4	5	6		
Questão n.º3: Considera que a GNR tem contribuído de forma eficaz para que as provas obtidas (âmbito da PD) na investigação sejam validadas?								
Segmento 3a	-	X			X		2	33,3%
Segmento 3b	-	X		X	X		3	50%
Segmento 3c	-	X					1	16,7%
Segmento 3d	-		X		X		2	33,3%
Segmento 3e	-			X		X	2	33,3%

Fonte: Elaboração própria.

3.3.4. Análise de Conteúdo à Questão 4

A tabela 8 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 4: “Considera que as qualificações da estrutura de IC da GNR se encontram ajustadas à obtenção de PD?”.

A primeira grande conclusão retirada é que as qualificações da estrutura da GNR ainda não se encontram ajustadas à obtenção de PD, visto que 50% dos entrevistados o revelam explicitamente. Por outro lado, Verdelho (2016) assume, com experiência nas várias reuniões com oficiais da estrutura de IC da GNR, que há uma grande sensibilidade e vontade em desenvolver estas qualificações na GNR.

Considerando a ligação entre a questão das qualificações e a formação, Machado (2016) aborda também a questão referindo que os cursos de IC estão a ser alvo de remodelação para introduzir o tema da PD.

Mais uma vez é abordada a questão de que se trata de um tema transversal a grande parte da GNR e, como tal, é apontado como objetivo idealístico ter todos os militares com formação nesta área, pese embora nem todos tenham de estar capacitados para recolher PD, pois essa não é a função do comum militar da GNR, integrado no dispositivo territorial. Para a função de recolha de PD, deve a GNR criar capacidades para poder fazer essa recolha em tempo útil. Neste âmbito, salienta-se o contributo de Cardoso (2016), referindo que cada NIC deve ter militares capacitados para fazer essa pesquisa e recolha de

PD e Pinho (2016) aponta para a criação de equipas móveis nos CTer, vocacionadas para fazer essa recolha de prova.

Tabela 8: Análise Qualitativa e Quantitativa das Respostas à Questão n.º4.

Segmentos das Respostas	Entrevistados						Frequência (n)	Percentagem (%)
	1	2	3	4	5	6		
Questão n.º4? Considera que as qualificações da estrutura de IC da GNR se encontram ajustadas à obtenção de PD?								
Segmento 4a	X						1	16,7%
Segmento 4b	X						1	16,7%
Segmento 4c		X	X		X		3	50%
Segmento 4d				X		X	2	33,3%
Segmento 4e						X	1	16,7%

Fonte: Elaboração própria.

3.3.5. Análise de Conteúdo à Questão 5

A tabela 9 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 5: “Considera que aos investigadores da GNR tem chegado conhecimento suficiente de novos métodos de investigação e de obtenção de PD?”. Tratando-se de um tema em constante evolução, em que estão sempre a surgir novos equipamentos e novas formas de se cometerem os crimes. Pretende-se, com esta questão, saber se a GNR também se adapta a esta realidade.

Seguindo as ideias explanadas nas perguntas anteriores, também nesta questão conclui-se que apenas em alguns CTer existe este cuidado de formação contínua no âmbito da PD, sendo reconhecida a importância de se fazer esse esforço. Na opinião de Botas (2016), para além de concordar que apenas nos distritos de Aveiro e Coimbra se verifica a existência de um esforço maior para esta formação, refere também que a GNR, enquanto instituição, se vai adaptando e realça como problema a velocidade dessa adaptação.

Embora não dê resposta cabal à pergunta, foi passada também a ideia, por 33,3% dos entrevistados, que estes novos métodos de investigação são um desafio constante e muito difícil de concretizar para qualquer órgão envolvido na atividade de IC.

De uma perspetiva centrada somente na componente criminalística da GNR, Vivas (2016) refere a pesquisa contínua de novos métodos de análise e extração de dados como uma das características inerentes aos examinadores e sem ela não conseguem cumprir as

suas funções. Isto porque diariamente são lançados para o mercado novos produtos e, portanto, os examinadores responsáveis pela extração de dados têm necessariamente de estar atualizados para cumprir a sua missão.

Tabela 9: Análise Qualitativa e Quantitativa das Respostas à Questão n.º5.

Segmentos das Respostas	Entrevistados						Frequência (n)	Porcentagem (%)
	1	2	3	4	5	6		
Questão n.º5: Considera que aos investigadores da GNR tem chegado conhecimento suficiente de novos métodos de investigação e de obtenção de PD?								
Segmento 5a	-	X			X		2	33,3%
Segmento 5b	-		X			X	2	33,3%
Segmento 5c	-		X			X	2	33,3%
Segmento 5d	-			X			1	16,7%
Segmento 5e	-				X	X	2	33,3%

Fonte: Elaboração própria.

3.3.6. Análise de Conteúdo à Questão 6

A tabela 10 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 6: “Aquando da necessidade da realização de exames forenses para obtenção de PD, já contou com o apoio dos laboratórios da GNR? Esse contributo foi dado de forma eficaz?”. Importa salientar que dois dos entrevistados nunca tiveram contacto com os laboratórios da GNR.

Dos entrevistados com experiência na colaboração com os laboratórios da GNR, quase todos são da opinião que esse contributo é eficaz. Vivas (2016) salienta que os processos com a intervenção do NTP de Coimbra têm uma elevada taxa de condenações. Botas (2016) afirma tratar-se de uma capacidade muito importante para o nosso sistema judicial pois o Laboratório de Policia Criminal da PJ tem dificuldade em dar resposta as todas as solicitações no âmbito dos exames forenses e perícias de PD. Pinho (2016) revela haver ainda aspetos a melhorar e ter de haver um trabalho contínuo. Nomeadamente deve haver uma melhor comunicação entre os órgãos da GNR para se poder fazer uma seleção mais criteriosa da informação relevante para os processos.

Tabela 10: Análise Qualitativa e Quantitativa das Respostas à Questão n.º6.

Segmentos das Respostas	Entrevistados						Frequência (n)	Porcentagem (%)
	1	2	3	4	5	6		
Questão n.º6: Aquando da necessidade da realização de exames forenses para obtenção de PD, já contou com o apoio dos laboratórios da GNR? Esse contributo foi dado de forma eficaz?								
Segmento 6a	-	-	X				1	16,7%
Segmento 6b	-	-		X	X	X	3	50%
Segmento 6c	-	-			X		1	16,7%

Fonte: Elaboração própria.

3.3.7. Análise de Conteúdo à Questão 7

A tabela 11 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 7: “Considera que os relatórios de resultados das provas (âmbito da PD), elaborados pelos investigadores da GNR, contribuem de forma eficaz para a validação das provas?”. A esta pergunta obteve-se 4 respostas.

Das repostas obtidas quase todas são de opinião positiva sobre os relatórios de resultados elaborados pela GNR, por contribuírem de forma eficaz para a validação das provas em julgamento. Em contrapartida, Pinho (2016) refere ser importante a apresentação dos relatórios devendo, contudo, evoluir-se no sentido de também ser apresentado na forma digital e não haver a tendência de apresentar os relatórios sob a forma de documentos impressos.

Tabela 11: Análise Qualitativa e Quantitativa das Respostas à Questão n.º7.

Segmentos das Respostas	Entrevistados						Frequência (n)	Porcentagem (%)
	1	2	3	4	5	6		
Questão n.º7: Considera que os relatórios de resultados das provas (âmbito da PD), elaborados pelos investigadores da GNR, contribuem de forma eficaz para a validação das provas?								
Segmento 7a	-	X		X	-	X	3	50%
Segmento 7b	-		X		-		1	16,7%

Fonte: Elaboração própria.

3.3.8. Análise de Conteúdo à Questão 8

A tabela 12 resume, da perspetiva qualitativa e quantitativa, as respostas dadas à questão n.º 8: “Quais as principais lacunas/ prioridades da GNR para a obtenção de PD?”. Dada a interligação entre as questões, as ideias acabam por se repetir o que dá mais força às conclusões que se podem retirar.

A totalidade dos entrevistados refere haver falta de formação nesta área sendo uma grande lacuna e, como tal, deve ser vista como uma prioridade para a GNR. Consta-se então que a formação tem de ser vista aqui como uma peça basilar pois está aliada a tudo o resto. Sem formação será mais lenta a adaptação do dispositivo quer ao conhecimento e constante atualização da legislação quer os conhecimentos técnicos de manuseamento dos equipamentos. Para além disto, Botas (2016) também revela que a falta de procedimentos não ajuda a que haja uma uniformização em toda a GNR.

Metade dos entrevistados aponta no sentido da GNR criar capacidades para ter militares com conhecimentos técnicos para fazer a recolha de PD em tempo útil e em todo o país. Realça-se aqui o contributo de Pinho (2016) naquilo que diz respeito à criação de equipas móveis em todos os CTer, de primeira resposta, para recolha de PD em sistemas informáticos simples, como é o caso dos smartphones. O entrevistado refere em vários momentos da entrevista ser um passo obrigatório para as polícias nacionais permitindo, se estas estruturas forem criadas, conseguir libertar as estruturas concebidas para o 2.º e 3.º níveis de recolha de prova pois, muitas vezes, estes trabalham nos níveis abaixo, ficando assim sobrecarregados e com dificuldades em dar resposta a todas as solicitações. O mesmo entrevistado refere, como objetivo mais difícil de conceber pois exige um esforço financeiro maior, a criação de mais estruturas para o 2.º nível de recolha de PD, ou seja, a criação de mais NTP com a capacidade de fazer exames forenses a sistemas informáticos, mais concretamente nos CTer com índices criminais mais elevados. Acompanhando este esforço de formação e de capacitações da GNR para a recolha de PD não pode deixar de haver também investimento equipamentos próprios para esta atividade (referido por 50% dos entrevistados).

É apontada também como lacuna na GNR, a falta de uma estratégia bem definida nesta área para permitir uma evolução mais rápida e padronizada. Para além disto, é referido que as capacidades criminalísticas da GNR devem ser dadas a conhecer não só aos magistrados do MP, mas também dentro da própria instituição.

Tabela 12: Análise Qualitativa e Quantitativa da Respostas à Questão n.º8.

Segmentos das Respostas	Entrevistados						Frequência (n)	Percentagem (%)
	1	2	3	4	5	6		
Questão n.º8: Quais as principais lacunas/ prioridades da GNR para a obtenção de PD?								
Segmento 8a	X	X	X	X	X	X	6	100%
Segmento 8b		X	X		X		3	50%
Segmento 8c			X				1	16,7%
Segmento 8d			X	X		X	3	50%
Segmento 8e					X		1	16,7%
Segmento 8f					X	X	2	33,3%
Segmento 8g					X		1	16,7%
Segmento 8h					X	X	2	16,7%

Fonte: Elaboração própria.

3.3.9. Análise de Conteúdo à entrevista efetuada ao NTP Coimbra

Foi aplicada uma diferente entrevista ao NTP Coimbra tendo em vista perceber quais são as suas principais capacidades e dificuldades, no âmbito da sua atividade de realização de exames forenses. Como se trata de uma entrevista isolada e com um guião diferente das anteriores a análise à mesma será meramente qualitativa, salientando os aspetos mais importantes e não recorrendo assim a tabelas. Assim, toda a informação que aqui referimos foi obtida através da entrevista, acompanhada de uma visita às instalações do NTP Coimbra⁴⁴.

Em termos de capacidades, o NTP Coimbra consegue atuar em 3 principais áreas (Rodrigues, 2016):

- Dispositivos móveis (telemóveis/ smartphones e GPS);
- Computadores, tablets, dispositivos de armazenamento e outros;
- Apreensão de dados online em servidores.

A divisão aqui definida não é estanque, mas prende-se essencialmente com o tipo de programas informáticos usados para a extração de dados. Para o primeiro grupo de dispositivos são usadas essencialmente, neste momento, ferramentas como o “Access Data Mobile Phone Examiner” e o “UFED 4PC”. Para o segundo grupo são essencialmente usados os programas de análise forense “Belkasoft Evidence Center” e “Access Data FTK.

⁴⁴ Vide Apêndice H.

Por fim, para a apreensão de dados online também são usados programas específicos como o “X Ways Forensics” e o “OS Triage”.

É importante também referir a existência de três formas para extrair a informação dos equipamentos: extração física, por sistemas de ficheiros e por extração lógica. A extração física permite recuperar ficheiros apagados e permite também ultrapassar seguranças, constituindo-se o tipo de extração a privilegiar. Existem dois tipos de extração física: através de “*boot loader*”, em que é possível aceder ao dispositivo pelo sistema operativo e, normalmente é por esta via que se consegue mais informação; e por Android Debug Bridge (ADB), à semelhança da mesma forma que se pode aceder a um dispositivo através de uma porta como a Universal Serial Bus (USB). Na extração por sistema de ficheiros poderá obter-se ficheiros apagados, mas não é possível fazer uma pesquisa tão profunda sendo que também não é possível ultrapassar seguranças. Na extração lógica, acede-se apenas aos ficheiros disponíveis para o utilizador no sistema e não é possível ultrapassar seguranças.

Deve-se salientar que, na extração de dados dos dispositivos, são usados bloqueadores de escrita, tratando-se de equipamentos concebidos para os examinadores fazerem pesquisas de dados sem qualquer alteração aos mesmos, preservando assim a integridade da informação.

A principal dificuldade apontada por Rodrigues (2016), no âmbito da atividade do NTP Coimbra, está ao nível do equipamento. Existe uma necessidade de renovar a frota de computadores porque o NTP trabalha com equipamentos já obsoletos. Há então necessidade de acompanhar a evolução tecnológica e também o crescente aumento de solicitações verificadas ao nível de pedidos de exame forense. Outra debilidade identificada refere-se à capacidade de resposta. Em 2015, o período de reposta aos pedidos de exame forense tinha uma duração máxima de dois meses. No que respeita ao ano corrente (2016), esse período de espera será ainda maior visto considerando que à data da entrevista o NTP Coimbra já realizou 517 exames forenses e tem mais de 600 exames pendentes, revelando estar a aumentar o número de solicitações de ano para ano.

3.4. Análise dos Questionários

Neste subcapítulo apresentam-se os resultados do questionário distribuído por todos os chefes de núcleos IC, da componente territorial, a nível nacional. As respostas ao questionário contribuem para determinar as capacidades e as dificuldades dos investigadores, tendo em vista a questão central do trabalho e visando, por sua vez, determinar a importância da PD para os inquéritos delegados pelo MP à GNR. Os gráficos que espelham os resultados das respostas às questões de conteúdo (grupo 3, questões 1 e 2) estão expostos nos Apêndices I e J.

A questão n.º 1 visa avaliar a frequência do acontecimento das situações descritas nas afirmações. A questão 1.1 é uma das mais importantes do questionário, pois pretende-se saber com que frequência existe necessidade de obter informação contida em dispositivos eletrónicos, no âmbito das investigações levadas a cabo pelos núcleos IC. Concluiu-se que a PD tem uma grande relevância para os inquéritos judiciais delegados na generalidade nos núcleos IC da GNR, visto que 34,1% dos inquiridos responde “Às Vezes” e 53,4% responde “Frequentemente”.

A este propósito especificou-se um pouco mais, a fim de determinar a importância da PD para os inquéritos delegados na perspetiva de cada tipo de núcleo IC, como pode ser consultado na tabela 13. Os tipos de núcleos onde é mais evidente esta importância da PD para as investigações são, sem margem para dúvida, os NIC e os NIAVE. Das 46 respostas obtidas dos chefes de NIC, 67,4% respondem “Frequentemente” e 23,9% responde “Às vezes”. É de salientar que é também nos NIC onde surgem as únicas respostas no sentido de haver sempre PD envolvida nos inquéritos, somando um total de 2 respostas na categoria “Sempre”, não havendo qualquer resposta na categoria “Nunca”. Das 15 respostas obtidas dos chefes dos NIAVE, 46,7% respondem “Frequentemente”, sendo que a percentagem é igual para a resposta “Às vezes” e apenas 4,3% responde “Raramente”. Embora os números sejam mais expressivos para os NIC e NIAVE, é de salientar que os restantes chefes de Núcleos IC também dão importância a este tipo de prova, não havendo nenhum tipo de núcleo que ponha de parte a obtenção de PD para os inquéritos, pois as percentagens de respostas “Nunca” e “Raramente” são sempre mais baixas para qualquer tipo de núcleo.

Tabela 13: Necessidade de obter PD em inquéritos por tipo de núcleo IC.

	NAO		NIAVE		NIC		NICAV		NICCO		NICCOA		Total Global	
	Nº	%	Nº	%	Nº	%	Nº	%	Nº	%	Nº	%	Nº	%
Nunca	1	11,1%	0	0%	0	0%	1	11,1%	0	0%	0	0%		
Raramente	1	11,1%	1	6,7%	2	4,3%	0	0%	1	25%	2	40%		
Às Vezes	4	44,4%	7	46,7%	11	23,9%	5	55,6%	2	50%	1	20%		
Frequentemente	3	33,3%	7	46,7%	31	67,4%	3	33,3%	1	25%	2	40%		
Sempre	0	0%	0	0%	2	4,3%	0	0%	0	0%	0	0%		
Total	9	100%	15	100%	46	100%	9	100%	4	100%	5	100%	88	100%

Fonte: Elaboração própria.

Com a questão 1.2 pretende-se saber com que frequência há necessidade de apreender dispositivos eletrônicos, para obtenção de PD, no decorrer de buscas. Grande parte dos inquiridos respondeu “Frequentemente” e “Às Vezes” com, respetivamente, 44,3% e 32,9% das respostas. As percentagens de respostas “Nunca”, “Raramente” e “Sempre” são muito reduzidas pelo que, conclui-se que a PD é um tipo de prova que carece de especial importância no decorrer de buscas e que os investigadores já estão despertados para esta realidade.

Com a questão 1.3 pretende-se saber com que frequência é solicitado, pelos investigadores da GNR, mandados de busca e pesquisa em dispositivos eletrônicos/redes de computadores. Nesta questão, as respostas “Nunca” e “Raramente” já têm uma maior expressão, relativamente às questões anteriores, com 10,2% e 17,1%, respetivamente. Ainda assim, as respostas “Frequentemente” e “Sempre” têm uma expressão maior, com 12,5% e 26,1%, respetivamente. A resposta “Às vezes” é a que se repete mais, com 34,1%. Neste ponto de vista, os resultados obtidos com esta questão surpreenderam pela positiva pois, esperava-se obter mais respostas negativas.

Relativamente à questão 1.4, conclui-se que os investigadores analisam, com muita frequência, PD após a extração da mesma. Mais concretamente, obteve-se 40,9% de respostas “Sempre”, sendo que as percentagens de respostas “Nunca” e “Raramente” são muito reduzidas. As respostas obtidas a esta questão acentuam o papel do investigador no âmbito da obtenção de PD, ou seja, a sua função não é saber fazer a recolha em si, mas sim perceber o resultado dessa extração e aproveitá-lo para o inquérito.

No presente questionário foram feitas algumas questões no sentido de perceber um pouco como funciona a articulação entre as diferentes vertentes de IC da GNR (operativa, criminalística e análise), como é o caso da questão 1.5 e da questão 1.6. Embora o objeto de estudo não seja perceber como se articulam os vários órgãos, construíram-se estas questões com o intuito de tentar perceber alguma falha ou lacuna para a obtenção de PD, tal como perceber a importância da PD para as várias vertentes de IC. Posto isto, a questão 1.5 tem como objetivo perceber com que frequência os investigadores sentem necessidade do apoio dos analistas, para a respetiva análise das provas. Aqui, as respostas apresentam percentagens muito uniformes, a rondar os 25%, com a exceção da resposta “Sempre” (3,4%), pelo que a PD também se afigura de alguma importância para a vertente de análise, no entanto, a maior parte dos inquiridos é da opinião de não sentir necessidade de se socorrer desta vertente de IC. A questão 1.6 visa então perceber com que frequência os investigadores se apoiam na componente criminalística da GNR para a pesquisa e apreensão de dispositivos eletrónicos. Aqui as respostas “Nunca”, “Raramente” e “Às Vezes” assumem claramente uma expressão muito grande, com 32,9%, 29,6% e 20,5%. Pode assim concluir-se que os investigadores, de uma forma geral, não se apoiam muito na componente criminalística para a pesquisa e apreensão de dispositivos eletrónicos.

A questão n.º 2 visa avaliar o grau de concordância com as afirmações apresentadas. As questões 2.1 e 2.2 têm como objetivo avaliar a formação dos militares relativamente ao tema da PD. Os resultados são completamente explícitos, revelando que, na opinião dos investigadores, a sua formação não está adequada às especificidades de pesquisa e apreensão de PD e, como tal, sentem haver necessidade de formação específica sobre este tema.

As questões 2.3 e 2.4 têm como objetivo perceber de que forma os investigadores da GNR se encontram familiarizados com as normas processuais aplicáveis à PD, nomeadamente às normas constantes na LC. Relativamente ao conhecimento das situações e formalidades a cumprir para fazer uma pesquisa num dispositivo eletrónico, questionada na questão 2.3, 42% dos inquiridos responderam “Concordo”, ainda assim, as percentagens de respostas “Discordo Totalmente” (4,5%), “Não Concordo” (22,7%) e “Não Concordo Nem Discordo” (16,3%). Embora cada uma por si não tenha grande expressão, mas a soma das suas percentagens revela um valor preocupante, por se verificar uma percentagem considerável de falta de familiaridade com esta legislação. Quanto à questão 2.4, relativa ao conhecimento das formas de apreensão de dados digitais, a conclusão tirada é em tudo idêntica ao que referimos na questão 2.3 pois os valores são muito parecidos.

A questão 2.5 está orientada para saber se os investigadores estão tecnicamente aptos ao nível dos procedimentos de manuseamento dos dispositivos eletrónicos que permitem a preservação das provas. A resposta a esta questão revelou-se muito uniforme pois as percentagens das respostas “Discordo Totalmente” (3,4%) e “Concordo Totalmente” (10,2%) têm percentagens mais baixas, comparando com as restantes categorias de resposta, que se aproximam todas dos 30%. Na interpretação dos resultados, a falta de procedimentos definidos na GNR para a recolha de PD contribui bastante para que os resultados não sejam os ideais.

A questão 2.6 visa precisamente saber se, quando surgem dúvidas técnicas, os investigadores recebem apoio da estrutura de IC, sendo as categorias de resposta centrais a apresentar percentagens muito parecidas e perto dos 30%. Ou seja, cerca de metade dos inquiridos refere não existir o apoio devido da estrutura de IC da GNR. Trata-se com certeza de um dos aspetos a melhorar dentro da GNR.

A questão 2.7 vem constatar, de facto, que a GNR não tem o equipamento necessário e adequado para fazer recolha de PD, visto que a esmagadora maioria das respostas dos inquiridos aponta nesse sentido, com 26% das respostas “Discordo Totalmente” e 42% “Não Concordo”, não havendo qualquer resposta para a opção “Concordo Totalmente”.

A questão 2.8 tem como objetivo perceber se a vertente de análise contribui para a investigação, fazendo a respetiva análise das provas. Aqui, as respostas “Não Concordo Nem Discordo” e “Concordo” são as que têm maior expressão, com 28,4% e 39,8%, respetivamente. As respostas “Discordo Totalmente” e “Concordo Totalmente” apresentam percentagens muito baixas. Constata-se assim que a PD tem grande importância para a vertente de análise, e que, de uma forma geral, os NAIIC têm um contributo muito ativo na análise de PD.

A questão 2.9 visa perceber se os investigadores têm conhecimento das capacidades criminalísticas da GNR no âmbito da recolha de PD. Embora a maior parte das respostas dos inquiridos aponte no sentido de conhecerem estas capacidades, a soma das percentagens das respostas “Discordo Totalmente”, “Não Concordo” e “Não Concordo Nem Discordo” é igual a 31,8%, o que revela ser importante haver uma maior divulgação dentro da própria GNR das suas capacidades criminalísticas para a obtenção de PD.

A questão 2.10 visa perceber se, no âmbito da atividade de IC, existe partilha de informação entre os vários órgãos da estrutura de IC da GNR. Metade dos inquiridos concordam com a afirmação e, juntando as percentagens dos inquiridos que não

concordam nem discordam e aqueles que concordam totalmente, revela que, de uma forma geral, a informação circula entre os vários órgãos da estrutura de IC, contribuindo assim para o sucesso das investigações.

As duas últimas questões visam perceber se existem problemas ao nível da articulação com as AJ e se estas estão sensibilizadas para o tema da PD. Uma vez que as respostas obtidas às questões 2.11 e 2.12 têm percentagens muito grandes nas categorias de resposta centrais, não nos permite retirar conclusões. Constata-se que as respostas com maior percentagem apontam no sentido das AJ encontrarem-se sensibilizadas para o tema e existir agilidade na relação entre estes e os investigadores para a obtenção de prova.

CONCLUSÕES E RECOMENDAÇÕES

O presente capítulo tem como objetivo tecer as conclusões do trabalho. Desta forma, começa-se por apresentar as respostas às QD e, por conseguinte, é apresentada a resposta à QP. É também no presente capítulo que são verificadas as HI. As respostas às questões de investigação, bem como a verificação das HI, são apoiadas, essencialmente, no trabalho de campo, apresentado no capítulo 3.

Começando pela QD1: “Quais as capacidades e dificuldades dos núcleos IC na obtenção de PD?”, demonstra-se com base na análise documental, através da qual foi elaborada a figura 2 e o Apêndice E, que a grande maioria dos CTer já contribuem para a obtenção de PD. Isto porque os seus núcleos IC têm inquéritos delegados pelo MP nos quais foram solicitados exames forenses para recolha de PD. Concluímos também, a este nível, que os vários núcleos IC a nível nacional não se encontram todos capacitados e despertos de igual forma para a obtenção de PD, pois, com base nos referidos gráficos, facilmente observa-se o grande desfasamento de resultados existentes entre os CTer com mais pedidos de exame forense, nomeadamente os CTer de Coimbra, Porto e Aveiro, e aqueles com menos pedidos de exame, de entre os quais evidenciam-se os CTer de Bragança, Castelo Branco, Açores e Madeira, sem qualquer pedido de exame forense no âmbito da recolha de PD.

Quanto ao tipo de núcleo IC, encontram-se mais capacitados e despertos para a obtenção de PD os NIC, os NAO e os NIAVE, isto referente à componente operativa da IC. Posto isto, e verificando também os resultados dos questionários aplicados aos chefes de núcleos IC deduz-se, quanto à determinação das capacidades da componente operativa de IC da GNR, que uma das principais capacidades dos núcleos IC consiste na solicitação de mandados de busca e apreensão para obtenção de PD. Neste âmbito, outra capacidade dos núcleos IC, é a análise das respetivas provas após recolhidas, de forma a perceber o conteúdo e a sua importância para os processos. No que diz respeito à determinação das dificuldades dos núcleos IC para a obtenção de PD, conclui-se que a falta de formação nesta área é determinante. Da falta de formação advêm outras dificuldades como a falta de capacidades técnicas para fazer uma pesquisa e recolha de PD e também o pleno conhecimento das normas específicas aplicáveis a este tipo de prova. Por último, os núcleos IC também não se encontram dotados de equipamento adequado para a recolha de PD. Para finalizar a QD1, resta verificar a H1: “Os núcleos IC não orientam a sua atividade

para obtenção de PD”. Dadas as conclusões referidas, pode-se afirmar já existir alguma sensibilidade por parte dos núcleos IC para a obtenção de PD, sendo que a sua atividade IC ainda não se encontra, de todo, ajustada à obtenção de PD. Contudo, ainda não lhes foram dadas capacidades por parte da própria estrutura da GNR para os núcleos poderem desenvolver-se mais nesta área, isto tendo em conta todas as dificuldades supra apresentadas.

Passando agora a responder à QD2: “Quais as capacidades e dificuldades da componente criminalística da GNR, na realização de exames forenses, para extração de PD?”. Constata-se que a GNR tem capacidade para realizar exames forenses a um grande conjunto de TIC, permitindo assim a recolha de PD. Nas TIC destacam-se os telemóveis, tratando-se da categoria definida na presente investigação examinada na grande maioria dos inquéritos. Mas estas capacidades vão muito para além dos telemóveis e, basicamente, a componente criminalística da GNR encontra-se dotada de laboratórios, mais concretamente o NTP de Coimbra e a RAFD de Alcabideche, capacitados para fazer a recolha de PD num grande espectro de dispositivos eletrónicos em que possa ser armazenada informação sob a forma de bits e bytes, desde computadores, dispositivos GPS, tablets, extração de metadados de correio eletrónico, cameras de filmar ou fotografar, etc. A capacidade de extração de PD dos equipamentos é efetuada através de computadores, equipamentos especiais (como é o exemplo dos bloqueadores de escrita) e também aplicações informáticas forenses específicas e adaptadas para cada tipo de dispositivo eletrónico. A criminalística da GNR consegue fazer os exames forenses por três vias, destacando-se a extração física. Salienta-se esta capacidade, não só por ser a mais usada, mas também por ser a forma de exame que permite obter mais informação, conseguindo ultrapassar seguranças do sistema operativo (palavras chave) e também por ser possível recuperar ficheiros apagados. As outras duas formas de exames são por sistema de ficheiros e por extração lógica. Por sistema de ficheiros não é possível fazer uma pesquisa tão profunda, mas permite recuperar ficheiros apagados, embora não permita ultrapassar seguranças. Através da extração lógica apenas é possível aceder aos ficheiros disponíveis ao utilizador do sistema operativo, não sendo possível obter ficheiros apagados nem ultrapassar seguranças. Ao nível das dificuldades da componente criminalística para recolha de PD, conclui-se essencialmente que estas se encontram a três níveis. Em primeiro lugar, há necessidade de acompanhar a crescente solicitação de pedidos de exame forense e do desenvolvimento das TIC renovando os equipamentos e adquirindo assim uma frota de computadores compatível com esta atividade. Em segundo lugar, também

relacionado com a crescente solicitação de pedidos de exame forense, a GNR está a perder capacidade de resposta. Isto prende-se muito com o facto de a GNR ainda não estar capacitada para um “primeiro nível de recolha de PD”, o que permitiria ao segundo nível (de exame forense) ficar mais liberto para a recolha de prova mais exigente ao nível da especialização e dos conhecimentos técnicos. Por último, os relatórios de resultados também são apontados como um aspeto a melhorar, devendo estes também ser exportados em formato digital e não em forma de documento impresso. Posto isto, verifica-se que a HI2, “A vertente criminalística da GNR tem capacidade para fazer a recolha de prova em qualquer dispositivo eletrónico”, é verdadeira.

Como última QD tem-se a QD3: “Quais os principais tipos de crime, da competência de investigação da GNR, associados à PD?” A resposta a esta questão é bastante objetiva pois esta decorre diretamente da análise da tabela 4 e do Apêndice D. Assim, de acordo com a tipificação feita no mapa para notação de crimes (Modelo 262), os crimes com maior expressão, no âmbito da PD, são o tráfico de estupefacientes e a violência doméstica contra cônjuges ou análogos, verificando-se assim a H3: “Os principais tipos de crime associados à PD são a violência doméstica contra cônjuges ou análogos e o tráfico de droga”. Para além destes crimes verificados nas hipóteses, pode também concluir que grande parte dos crimes obtidos nos resultados são crimes da competência de IC da GNR.

Dadas as respostas às QD, pretende-se agora responder à QP:” Qual a importância da PD nos inquéritos delegados pelo MP à GNR?” À medida que são tecidas as conclusões, são também feitas recomendações que são consideradas importantes na ótica do investigador. Em primeiro lugar, observa-se nos resultados das entrevistas, a importância da PD para a GNR justificada com o aumento da criminalidade que recorre às TIC e dos crimes em que é possível obter PD. Criminalidade essa que, em grande parte, é da competência de IC da GNR. Para reforçar esta ideia, a resposta à QD3 refere alguns tipos de crime com mais relevância no âmbito da PD. Torna-se assim importante que a IC da GNR priorize a PD para os inquéritos.

Com base nos resultados obtidos nas entrevistas, salienta-se a importância de uma adaptação da GNR por forma a conseguir orientar a sua atividade de IC para a obtenção de PD. Assim, torna-se importante remodelar a IC da GNR para criar estruturas que dividam a obtenção de PD em dois níveis. O primeiro nível pode muito bem centrar-se ao nível dos NIC dos DTer ou de algumas equipas móveis pertencentes aos CTer, responsáveis pela recolha de prova de menor complexidade, em sistemas informáticos mais simples, como é

o exemplo dos smartphones. Quanto ao segundo nível (nível de exame forense), é importante capacitar os órgãos da GNR (NTP's) para o fazer a nível regional, ou seja, funcionar como um complemento ao primeiro nível e para intervir nos casos de maior complexidade. A este nível, a ativação da RAFD, em 2016, permite alargar as capacidades da GNR neste âmbito, demonstrando capacidade de adaptação a esta realidade. Posto isto, através de alguns contributos das entrevistas, é perceptível ver o modelo de IC da GNR mais orientado para a obtenção de prova através de escutas telefónicas, de seguimentos e vigilância e também de inquirições. A este nível é também importante que a GNR adapte o seu modelo de investigação para acompanhar a evolução dos fenómenos criminais, que supõe cada vez mais conduzir esforços para a recolha de PD.

Para acompanhar tudo isto, é importante a GNR investir na área da formação sobre PD. Aponta-se como objetivo idealístico proporcionar a formação elementar sobre PD a todos os militares da GNR e, um pouco mais aprofundada a todos os militares da estrutura de IC. A formação deve ser contínua, pois trata-se de um tema em permanente evolução. É através da formação que se consolidam os conhecimentos técnicos e legais aplicáveis à obtenção de PD, sendo este saber indispensável para a IC da GNR.

A PD é um tipo de prova muito importante não só na fase de inquérito, mas também na aquisição da notícia de crime. Isto porque a PD é volátil, e como tal, deve ser identificada e recolhida assim que possível. Neste âmbito destaca-se a importância das MCP, pois é através destas medidas que se consegue acautelar a prova, o mais cedo possível, e simplificar um pouco as normais rotinas processuais. Esta teoria tem ainda mais força para um OPC como a GNR, pois, pelos resultados apresentados, é com certeza um dos que recebe mais participações criminais.

Outra vertente em que PD tem importância é no âmbito da cooperação policial para fins de IC. Como se pode constatar nos resultados, a GNR já contribuiu com exames forenses para recolha de PD em cooperação com o SEF. Considera-se não ser necessário a todos os OPC possuírem estas valências, até porque seria algo muito dispendioso. Como tal, é importante dar a conhecer as valências entre os vários OPC para rentabilizar ao máximo os meios de cada um, contribuindo assim para uma melhor eficácia e eficiência da IC. Para além de dar a conhecer valências aos vários OPC, é também importante fazê-lo dentro da própria instituição. Trata-se de uma questão abordada, ao nível do trabalho de campo, tanto nos inquéritos como nos questionários, concluindo que ainda deve ser mais explorada pela GNR.

Para finalizar, concluímos que a mudança dos fenómenos criminais associada ao crescente uso das TIC requer uma maior proatividade de um OPC como a GNR, no sentido de proporcionar capacidades e competências ao efetivo orientadas para a obtenção de PD. Como tal, a GNR deve ajustar a formação e adaptar a sua estrutura assemelhando-se às polícias mais desenvolvidas na área da PD, seguindo os melhores exemplos internacionais.

BIBLIOGRAFIA

- Academia Militar. (11 de maio de 2015). NEP 520/4.^a. *Normas de Execução Permanente*.
- Academia Militar. (20 de janeiro de 2016). NEP 522/1.^a. *Normas de Execução Permanente*.
- Assembleia da República. (02 de abril de 1976). Constituição da República Portuguesa.
- Assembleia da República. (14 de março de 1985). Decreto lei n.º 63/85, de 14 de março: Código do direito de autores e dos direitos conexos. *Diário da República, 1ª série, n.º 61*, pp. 662-689.
- Assembleia da República. (17 de fevereiro de 1987). Decreto lei n.º 78/87, de 17 de fevereiro: Código de Processo Penal. *Diário da República, 1ª série, n.º 40*, pp. 619-699.
- Assembleia da República. (22 de janeiro de 1993). Lei n.º 15/93, de 22 de janeiro: Legislação de Combate à Droga. *Diário da República, 1ª série, n.º 18*, pp. 234-252.
- Assembleia da República. (15 de março de 1995). Decreto lei n.º 48/95, de 15 de março: Código Penal. *Diário da República*.
- Assembleia da República. (06 de novembro de 2007). Lei n.º 63/2007, de 6 de novembro: Lei Orgânica da GNR. *Diário da República, 1ª série, n.º 213*.
- Assembleia da República. (27 de agosto de 2008). Lei n.º 49/2008, de 27 de agosto: Lei Orgânica da Investigação Criminal. *Diário da República, 1ª série, n.º 165*, pp. 6038-6042.
- Assembleia da República. (15 de setembro de 2009). Lei n.º 109/2009, de 15 de setembro: Lei do Cibercrime. *Diário da República, 1ª série, n.º 179*, pp. 6319-6325.
- Botas, C. (16 de maio de 2016). A importância da Prova Digital. (M. Mateus, Entrevistador)
- Branco, C. (2010). *Guarda Nacional Republicana - Contradições e Ambiguidades*. Lisboa: Edições Sílabo.
- Cardoso, R. (12 de maio de 2016). A importância da Prova Digital. (M. Mateus, Entrevistador)

- Centro Nacional de Cibersegurança. (s.d.). *Centro Nacional de Cibersegurança*. Obtido em 04 de abril de 2016, de <http://www.cncs.gov.pt/cert-pt/coordenacao-da-resposta-a-incidentes/index.html>
- Guarda Nacional Republicana. (21 de janeiro de 2014a). Despacho 18/14. *Ordem à Guarda*.
- Guarda Nacional Republicana. (11 de 03 de 2014b). *Diretiva Operacional n.º 01/14 - Orientações para implementação da estrutura de investigação criminL*.
- Machado, J. (16 de maio de 2016). A importância da Prova Digital. (M. Mateus, Entrevistador)
- Marconi, M. D., & Lakatos, E. M. (2003). *Fundamentos de Metodologia Científica* (5ª Edição ed.). São Paulo: Editora Atlas.
- Marques, P. P. (2013). *Informática Forense - Recolha e preservação de prova digital. Dissertação para a obtenção do grau Mestre em Segurança em Sistemas de Informação*. Lisboa: Universidade Católica Portuguesa - Faculdade de Engenharia.
- Mendes, P. (2014). *Lições de Direito Processual Penal*. Coimbra: Almedina.
- Procuradoria Geral da República. (09 de julho de 2012). *Nota prática n.º 1/2012, O endereço IP e a identificação do seu utilizador*. Obtido em 04 de abril de 2016, de Gabinete de Cibercrime: <http://cibercrime.ministeriopublico.pt/notas-praticas>
- Procuradoria Geral da República. (12 de junho de 2014a). *Nota prática n.º 3/2014, Pedidos de informações a fornecedores de serviços Internet dos Estados Unidos da América*. Obtido em 04 de abril de 2016, de Gabinete de Cibercrime: <http://cibercrime.ministeriopublico.pt/notas-praticas>
- Procuradoria Geral da República. (22 de dezembro de 2014b). *Nota prática n.º 4/2014, Pedidos de informações à Google, à Facebook e à Microsoft - experiência prática*. Obtido em 04 de abril de 2016, de Gabinete de Cibercrime: <http://cibercrime.ministeriopublico.pt/notas-praticas>
- Procuradoria Geral da República. (30 de dezembro de 2015a). *Nota prática n.º 7/2015, Retenção de dados de tráfego e Lei n.º 32/2008, de 17 de Julho*. Obtido em 04 de abril de 2016, de Gabinete de Cibercrime: <http://cibercrime.ministeriopublico.pt/notas-praticas>
- Procuradoria Geral da República. (01 de setembro de 2015b). *Plano de Ação do Ministério Público 2015 - 2016*. Obtido em 05 de abril de 2016, de Gabinete de Cibercrime: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/plano_acao_cibercrime_2015-2016.pdf

- Pinho, C. (13 de maio de 2016). A importância da Prova Digital. (M. Mateus, Entrevistador)
- Ramos, A. D. (2015). *A prova digital em processo penal: o correio eletrónico*. Lisboa: Chiado Editora.
- Rodrigues. (16 de maio de 2016). Capacidades e dificuldades do NTP Coimbra. (M. Mateus, Entrevistador)
- Sarmiento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.
- Soares, P. A. (2014). *Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia*. Coimbra: Almedina.
- Sistema de Segurança Interna. (2015). *Relatório Anual de Segurança Interna*. Lisboa.
- Scientific Working Group on Digital Evidence. (15 de novembro de 2004). *Guidelines & Recommendations for Training in Digital & Multimedia Evidence*. Obtido em 02 de maio de 2016, de SWGDE:
<https://www.swgde.org/documents/Archived%20Documents>
- Scientific Working Group on Digital Evidence. (13 de abril de 2013). *Digital & Multimedia Evidence Glossary*. Obtido em 02 de maio de 2016, de SWGDE:
<https://www.swgde.org/documents/Archived%20Documents>
- Verdelho, P. (2004). *A obtenção de prova no ambiente digital*. Lisboa: DIAP Lisboa.
- Verdelho, P. (novembro de 2015). *Cibercrime e Prova Digital*. Obtido de Unidade de Formação Jurídica e Judiciária do Observatório Permanente da Justiça Portuguesa:
http://opj.ces.uc.pt/unifoj/site/index.php?id=5824&id_lingua=1&pag=12730
- Verdelho, P. (10 de maio de 2016). A importância da Prova Digital. (M. Mateus, Entrevistador)
- Vivas, J. (13 de maio de 2016). A importância da Prova Digital. (M. Mateus, Entrevistador)

APÊNDICES

APÊNDICE A – Guião de Entrevista (Magistrados do MP e Oficiais da GNR)

Entrevistador: Miguel Ângelo Trindade Mateus

Bloco A: Caraterização do entrevistado

Nome:

Posto/Equivalente:

Cargo/Função:

Unidade:

Local:

Data:

Bloco B: Guião de perguntas

1. Considera ser relevante que a IC priorize a PD para os inquiridos?
2. Considera que as capacidades técnicas dos investigadores da GNR e as rotinas processuais são adequadas para a obtenção de PD?
3. Considera que a GNR tem contribuído de forma eficaz para que as provas obtidas (âmbito da PD) na investigação sejam validadas?
4. Considera que as qualificações da estrutura de IC da GNR se encontram ajustadas à obtenção de PD?
5. Considera que aos investigadores da GNR tem chegado conhecimento suficiente de novos métodos de investigação e de obtenção de PD?
6. Aquando da necessidade de realização de exames forenses para obtenção de PD, já contou com o apoio dos laboratórios da GNR? Esse contributo foi dado de forma eficaz?
7. Considera que os relatórios de resultados das provas (âmbito da PD), elaborados pelos investigadores da GNR, contribuem de forma eficaz para a validação das provas?
8. Quais as principais lacunas/prioridades da GNR para a obtenção de PD?

APÊNDICE B – Guião de Entrevista (NTP Coimbra)

Entrevistador: Miguel Ângelo Trindade Mateus

Bloco A: Caraterização do entrevistado

Nome:

Posto/Equivalente:

Cargo/Função:

Unidade:


Local:

Data:


Bloco B: Guião de perguntas

1. Descreva as capacidades do NTP Coimbra para a realização de exames?
2. Quais as principais dificuldades do NTP Coimbra para o cumprimento da sua missão?
3. Em média, quais os tempos de espera para a exportação dos exames pedidos?

APÊNDICE C – Questionários núcleos IC



Academia Militar
Guarda Nacional Republicana




Questionário Chefes Núcleos IC
Crimes em ambiente digital - Investigação da GNR para a obtenção de prova

1. 1. Apresentação


O presente inquérito por questionário surge no âmbito do Trabalho de Investigação Aplicada (TIA), necessário para a conclusão do Curso de Formação de Oficiais da Guarda Nacional Republicana. Esta investigação está subordinada ao tema "Crimes em ambiente digital – Investigação da GNR para a obtenção de prova" e é elaborada pelo Aspirante de Cavalaria da GNR Miguel Ângelo Trindade Mateus.

Neste âmbito, o presente inquérito por questionário tem como objetivos determinar as capacidades e dificuldades da componente operativa da Investigação Criminal (IC) da GNR e também determinar a importância da prova digital para os inquéritos delegados pelo Ministério Público e investigados pelos militares da GNR.

O questionário é dirigido a todos os chefes dos Núcleos IC da GNR, da vertente territorial. Os dados são anónimos e para utilização particular da presente investigação.



Academia Militar
Guarda Nacional Republicana



Questionário Chefes Núcleos IC
Crimes em ambiente digital - Investigação da GNR para a obtenção de prova

2. 2. Caracterização Sociodemográfica

1. Idade


2. Género

3. Habilitações literárias


4. Posto

5. Tipo de Núcleo IC

6. Anos de experiência na estrutura de IC



Academia Militar
Guarda Nacional Republicana



Questionário Chefes Núcleos IC
Crimes em ambiente digital - Investigação da GNR para a obtenção de prova

3. Importância da prova digital/ Capacidades e dificuldades dos Núcleos IC

Considere a seguinte definição para a resposta às questões:

Prova digital: Toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações.
Excerto de: Armando Dias Ramos. "A Prova Digital em Processo Penal: O correio eletrónico".

Considere dispositivos eletrónicos como computadores, telemóveis, dispositivos de armazenamento, tacógrafos digitais, GPS ou qualquer outro dispositivo que possa conter informação relevante para o inquérito.

1. Pretende-se, nesta questão, avaliar a frequência com que acontecem as situações descritas nas 6 afirmações apresentadas. Tenha em conta os inquéritos delegados pela Autoridade Judiciária (AJ) ao Núcleo IC por si chefiado.

Para cada afirmação, assinale o campo correspondente à resposta que melhor define a sua opinião, de acordo com a escala de Likert (Nunca; Raramente; Às Vezes; Frequentemente; Sempre):

	Nunca	Raramente	Às Vezes	Frequentemente	Sempre
1. Tem inquéritos em que sente necessidade de obter informação contida em dispositivos eletrónicos (prova digital).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. No decorrer de uma busca, tem necessidade de apreender dispositivos eletrónicos onde pode estar contida prova relevante para o inquérito.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Envia relatórios à AJ a solicitar mandados de busca e pesquisa em dispositivos eletrónicos/redes de computadores.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. Após extração da informação dos equipamentos, o núcleo IC analisa a informação para selecionar as provas relevantes para o inquérito.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. Tem sido necessária do apoio do Núcleo de Análise de Informações e Informação Criminal (NAIIC) para a análise da informação contida em dispositivos eletrónicos.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. Tem a necessidade do apoio do Núcleo Técnico Pericial (NTP) ou do Núcleo de Apoio Técnico (NAT) para apreensão dos dispositivos eletrónicos.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.

Pretende-se nesta questão avaliar o grau de concordância com as 12 afirmações apresentadas.

Para cada afirmação assinale o campo correspondente à resposta que melhor define a sua opinião, de acordo com a escala de Likert (Discordo Totalmente; Não Concordo; Não Concordo Nem Discordo; Concordo; Concordo Totalmente):


	Discordo Totalmente	Não Concordo	Não Concordo Nem Discordo	Concordo	Concordo Totalmente
1. A formação de IC que tem a adequada às especificidades de apreensão e pesquisa de prova digital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Discordo Totalmente	Não Concordo	Não Concordo Nem Discordo	Concordo	Concordo Totalmente
2. Os investigadores deveriam ter formação específica sobre prova digital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Tenho conhecimento das situações e das formalidades que tenho de cumprir para fazer uma pesquisa num dispositivo eletrónico, sem autorização prévia da AJ.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. Tenho conhecimento das formas de apreensão de prova digital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. Sei os procedimentos de manuseamento de dispositivos eletrónicos que permitem preservar a prova digital (situação de busca ou apreensão).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. O Núcleo IC recebe apoio técnico da Estrutura de IC da GNR quando surgem dúvidas técnicas para apreensão de dispositivos eletrónicos.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7. O Núcleo IC possui as ferramentas necessárias para fazer a apreensão e pesquisa em dispositivos eletrónicos.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8. O Núcleo IC tem a colaboração do NAIC para a análise de prova digital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9. Tenho conhecimento que a GNR possui NTP's com capacidade de análise forense a dispositivos eletrónicos.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10. Existe partilha de informação e colaboração entre as componentes de IC da GNR (operativa, de análise e criminalística).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11. As autoridades judiciais estão sensibilizadas para a temática da prova digital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5

	Discordo Totalmente	Não Concordo	Não Concordo Nem Discordo	Concordo	Concordo Totalmente
12. Existe agilidade na relação entre os investigadores e as autoridades judiciais para a obtenção de prova digital.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6



Academia Militar
Guarda Nacional Republicana



Questionário Chefes Núcleos IC
Crimes em ambiente digital - Investigação da GNR para a obtenção de prova

4. Agradecimento

Obrigado pela colaboração!

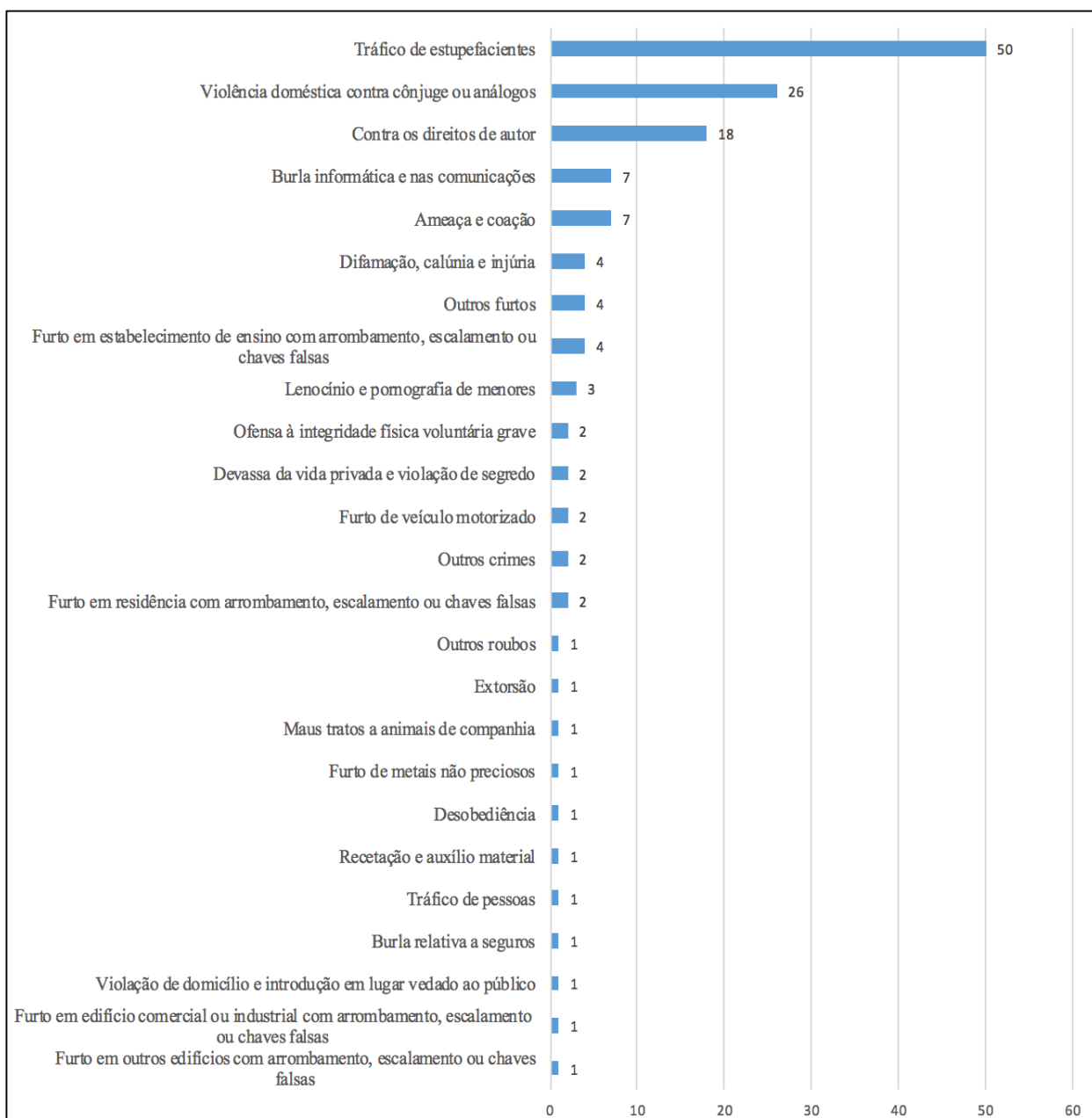
Cordiais cumprimentos,

Miguel Mateus
Aspirante de GNR Cavalaria

Clique em "concluído" para finalizar o questionário

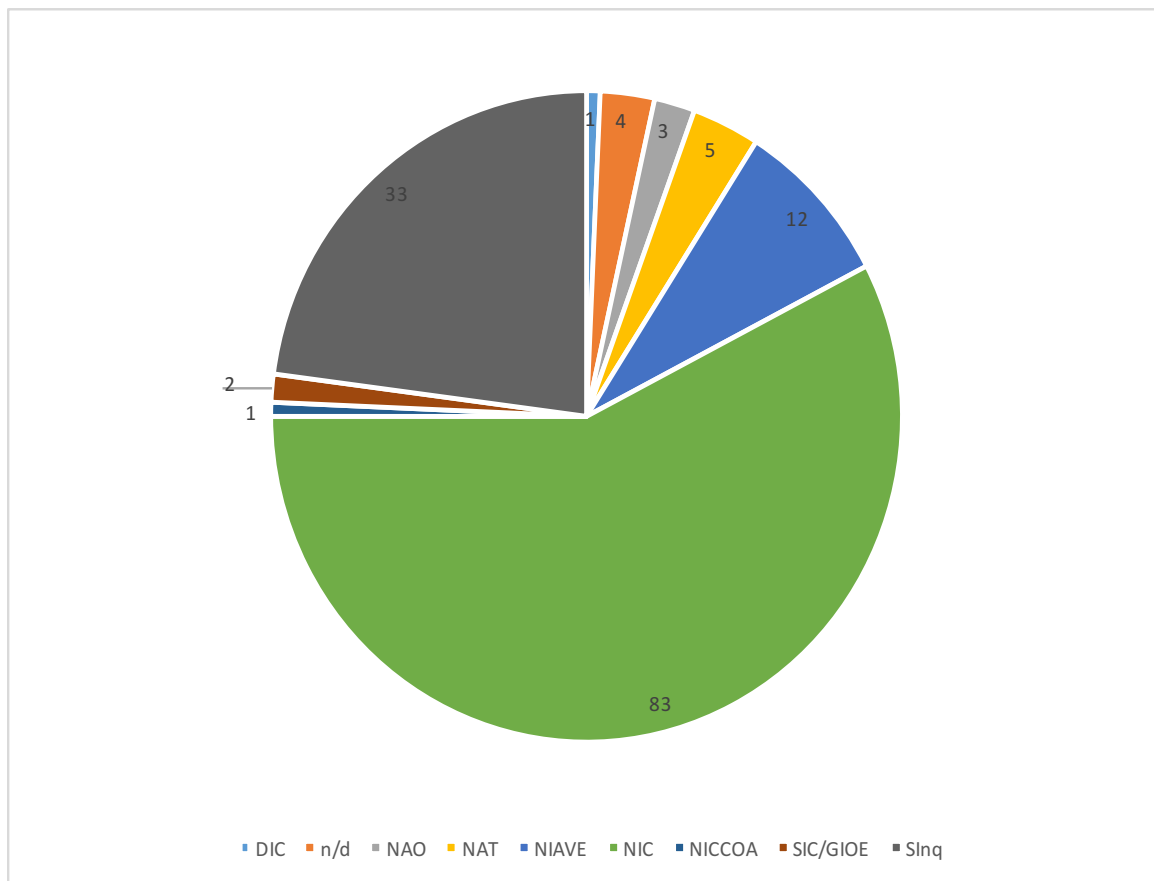
7

APÊNDICE D – Tipos de crime investigados nos inquéritos judiciais



Fonte: Adaptado de NTP Coimbra.

APÊNDICE E – Tipos de núcleo IC na origem dos pedidos de exame forense para obtenção de PD



Fonte: Adaptado de NTP Coimbra

APÊNDICE F – Lista de segmentos definidos

Questão n.º1	
Segmento 1a	Sim, a PD deve ser priorizada para os inquéritos
Segmento 1b	Criminalidade através dos meios informáticos e de comunicação tem vindo a aumentar
Segmento 1c	Crimes tradicionais têm uma grande expressão no que aos crimes cometidos através dos meio informáticos/comunicação diz respeito.
Questão n.º2	
Segmento 2a	As capacidades técnicas dos investigadores da GNR não se encontram ajustadas à obtenção de PD
Segmento 2b	A GNR está a adaptar-se no sentido de criar estruturas e formação para fazer face a esta realidade
Segmento 2c	No mínimo, todo o efetivo da estrutura de IC deveria ter formação sobre PD
Segmento 2d	Existe formação em alguns pontos do país
Segmento 2e	É importante ter os conhecimentos técnicos e os conhecimentos legais
Segmento 2f	Um guia de recolha de PD aplicável a todo o dispositivo da GNR seria uma boa forma de colmatar as algumas lacunas.
Segmento 2g	Não é função do investigador recolher a prova dos equipamentos mas sim perceber o resultado dessa recolha.
Segmento 2h	É fundamental tentar obter PD no momento da notícia do crime ou antes do 1º interrogatório judicial
Questão n.º3	
Segmento 3a	A GNR ainda não está vocacionada para a obtenção de PD, apoiando-se ainda muito noutros tipos de prova.
Segmento 3b	Militares da GNR devem ter perfeito conhecimento da LC, nomeadamente nas normas respeitantes à pesquisa e apreensão de dados
Segmento 3c	MCP têm grande importância para a obtenção de PD
Segmento 3d	A GNR não tem contribuído de forma eficaz
Segmento 3e	A vertente criminalística da GNR cumpre os requisitos necessários e contribui de forma eficaz

Questão n.º4	
Segmento 4a	Há uma grande sensibilidade e vontade por parte dos oficiais da estrutura IC da GNR em desenvolver qualificações da GNR
Segmento 4b	É um tema que deve ser abordado na formação inicial de Guardas não dispensando a devida formação contínua
Segmento 4c	As qualificações ainda não se encontram ajustadas
Segmento 4d	A vertente IC Criminalística da GNR está a fazer um investimento neste campo, ajustando assim as suas qualificações
Segmento 4e	4e- Os cursos de IC da GNR também estão a ser alvo de remodelação, introduzindo-se o tema da PD
Questão n.º5	
Segmento 5a	É um desafio constante e muito difícil de concretizar para todos os órgãos envolvidos na atividade de IC
Segmento 5b	Em algumas comarcas/CTer já existe formação neste sentido
Segmento 5c	É importante criar formação contínua ao nível da GNR para desenvolver essas capacidades de adaptação
Segmento 5d	É uma característica inerente à vertente da criminalística.
Segmento 5e	Embora a GNR se vá adaptando aos novos métodos de investigação essa adaptação é lenta
Questão n.º6	
Segmento 6a	Esse contributo pode ser melhorado
Segmento 6b	Esse contributo é eficaz
Segmento 6c	A capacidade de resposta é muito importante
Questão n.º7	
Segmento 7a	Os relatórios têm contribuído para a validação das provas
Segmento 7b	Os relatórios não devem ser apresentados sob a forma de prova documental

Questão n.º8	
Segmento 8a	Falta de formação transversal a todos os militares sobre o tema
Segmento 8b	Falta de militares com conhecimentos técnicos que possa atuar em tempo útil para a recolha de prova (1º nível de recolha de PD)
Segmento 8c	Falta de criação de estruturas para o 2º nível de recolha de PD (exame forense)
Segmento 8d	Necessidade de investimento em materiais próprios para esta atividade
Segmento 8e	Falta de procedimentos para recolha de PD
Segmento 8f	Desconhecimento das capacidades da vertente criminalística dentro da própria GNR
Segmento 8g	Falta de estratégia da própria instituição
Segmento 8h	Dar a conhecer ao MP as capacidades criminalísticas da GNR/ Saber quais as necessidades do MP para a produção de prova

APÊNDICE G – Análise das entrevistas

	Resposta à Q1 Considera ser relevante que a IC priorize a PD para os inquéritos?	Segmentos Identificados
E1	“Sem dúvida que a prova digital deve ser priorizada para os inquéritos.”	1a
	“De fato, aumentou o cibercrime em sentido estrito, mas os crimes cometidos através das redes de comunicação, como as burlas, injúrias, difamações, ameaças e outros, os chamados crimes tradicionais, e que são cometidos pelas redes de comunicação são muito mais e têm tendência para aumentar mais que os primeiros”	1b 1c
	“Os crimes tradicionais têm uma proporção muito maior do que os restantes”	1c
	“... mesmo os crimes tradicionais não cometidos pelas redes de comunicação também supõem, e cada vez mais, prova digital.”	1c
E2	“É cada vez mais frequente a necessidade de fazer recolha de prova em ambiente digital.”	1b
	“Isto ocorre em qualquer tipo de crime: desde crimes contra a honra, contra o património, contra a integridade física ou contra a vida”	1b 1c
	“A tendência para haver prova digital envolvida nos inquéritos será cada vez maior.”	1a 1b
E3	“Não é importante, é determinante.”	1a
	“... já estamos, no que à prova digital diz respeito, a assistir a um fenómeno que já não é do presente, muito menos do futuro, até já é do passado.”	1a 1b
	“... o problema maior está no âmbito dos crimes que são cometidos através de meios informáticos.”	1c
	“Isto significa que a criminalidade está a mudar. Não só em Portugal, mas sim no mundo inteiro. “	1c
	“... a criminalidade cometida através de meios informáticos, pese embora nem toda ela refletida nas estatísticas, tem vindo a aumentar.”	1b
“... mas é neste campo da prova digital que as demais forças policiais com competências de investigação criminal em processo criminal, nomeadamente a GNR, a PSP e outras, têm um campo de intervenção muito grande.”	1c	

E4	“...a investigação criminal não pode (nem deve) deixar de priorizar a prova digital em sede de inquérito criminal, sob pena de eventualmente perder a derradeira prova que irá ilibar ou condenar determinado suspeito (arguido), prova essa inalcançável por outro qualquer meio tradicional.”	1a
	“Existe efetivamente um aproveitamento por parte das pessoas que perpetuam e desenvolvem atividades ilícitas, das capacidades e potencialidades permitidas por estes novos meios de comunicação.”	1b
E5	“Trata-se de um tipo de prova com cada vez mais relevância e que é importante ser acautelada, principalmente em algumas tipologias criminais, em que os meios informáticos e de comunicações são usados como meio para poder praticar o crime, não só o crime em si.”	1a 1b 1c
E6	“Sim. É a evolução dos tempos.”	1a
	“Atualmente a criminalidade é feita utilizando a internet, quer seja pela comunicação, quer pela passagem de dados, independentemente do crime.”	1b 1c

Resposta à Q2		Segmentos Identificados
<p>Considera que as capacidades técnicas dos investigadores da GNR e as rotinas processuais são adequadas para a obtenção de PD?</p>		
E1	<p>“todos nos estamos a deparar com novas dificuldades porque não temos preparação. Vamos tendo aos poucos e estamos a avançar nesse sentido, tal como a GNR também o está a fazer.”</p>	<p>2a 2b</p>
	<p>“Como objetivo idealístico, todos os elementos que trabalham na investigação criminal deverão ter o mínimo de conhecimentos sobre prova digital.”</p>	2c
	<p>“O que existe são sessões de trabalho do MP, a nível local, em que existe total abertura para que os militares da GNR participem, como já o fizeram recentemente por duas vezes, em Portalegre e em Setúbal.”</p>	2d
	<p>“... não é expectável que o investigador em geral saiba extrair prova digital de um aparelho (...). A sua função é perceber o resultado dessa extração apurada.”</p>	2g
	<p>“A Prova digital não é conciliável com esta rotina processual, pois é volátil, o que quer dizer que se não se a tenta obter no início da investigação, quando mais tarde se vai tentar angariar prova, através de uma busca ou apreensão, esta já não está disponível.”</p>	2h
	<p>“... é no momento da notícia do crime que isto se deve detetar, e no momento em que a GNR ou a PSP recebem a notícia do crime deve haver alguma sensibilidade para isto.”</p>	2h
	<p>“é importante introduzir no circuito, e mudar a rotina por forma a que o militar da GNR que receber a queixa pergunte pelo email original, e creio que o comum militar da GNR que desempenha essa função ainda não está sensibilizado para tal.”</p>	2h
	<p>“... inclusivamente até para determinar questões indiciárias que podem ser relevantes para o interrogatório, que se não forem recolhidas através de pessoas especializadas neste nível se perdem”</p>	2h
E2	<p>“... a GNR ainda não está capacitada para fazer a recolha de prova digital.”</p>	2a
	<p>“... grande parte dos investigadores da GNR ainda não estão capacitados para fazer uma pesquisa num computador, de forma compatível com aquilo que são as boas práticas para a obtenção de prova digital.”</p>	2a
	<p>“... suponho que apenas em Coimbra haverá investigadores da GNR capacitados para tal”</p>	2b
	<p>“... muitas vezes, durante ou após a busca é necessário analisar telemóveis ou quaisquer outros dispositivos, para conseguir retirar informação que é decisiva para o primeiro interrogatório judicial.</p>	2h

E3	“Não, e isso tem muito a ver com o meu trabalho de há 2 anos para cá ...”	2a
	“... já fiz várias sessões de formação onde estiveram presentes elementos da GNR, para lhes dar a formação básica legal e também técnica de abordagem”	2d 2e
	“Nessas sessões foram explicados os requisitos legais e procedimentos, que estão condensados num guia que é norma na comarca de Aveiro – um guia de recolha de prova digital.”	2e 2f
	“Isto é absolutamente criterioso e fundamental fazer-se porque é neste nível também que se encontra aquilo que é formação que todos os militares da GNR devem ter.”	2c
	“Mas pelos menos aqueles conselhos básicos que se devem dar a uma pessoa que apresenta queixa ou coloca dúvidas no atendimento ao público ou num piquete, todos os militares devem estar capacitados para tal.”	2c 2e
E4	“Julgo que a GNR tem em toda a sua estrutura cerca de seis militares, todos eles da classe profissional de Guardas a trabalhar nesta temática.”	2b
	“Não só as capacidades não são adequadas como o número de especialistas nesta área fica aquém do necessário, atendendo ao volume de trabalho ao qual hoje em dia a GNR já tem de dar resposta.”	 2a
E5	“Ao existir um vazio de procedimentos na GNR, perdemos muita dessa capacidade técnica para a obtenção de prova digital.”	2f
	“Os nossos investigadores dos NIC e dos NIAVE, essencialmente, já estão a ficar cada vez mais despertos no sentido de acautelar esse tipo de prova, que muitas vezes se encontra em telemóveis e smartphones.”	2b
	“Os nossos investigadores ainda não se encontram muito orientados para este tipo de recolha de prova. “	2a
E6	“Está-se a iniciar formação nesse sentido. Já temos alguns investigadores, que por terem mais ocorrências, estão mais rotinados, em algumas SIC.”	2b

Resposta à Q3 Considera que a GNR tem contribuído de forma eficaz, para que as provas obtidas (âmbito da PD) na investigação sejam validadas?		Segmentos Identificados
E1	-	-
E2	“... atualmente os OPC ainda não estão verdadeiramente preparados para isto. Isto de uma forma geral, não quer dizer que em cada instituição não haja pessoas capacitadas para tal, pois aí haverá certamente.”	3a
	“Vamos ter que superar a forma de provar as coisas. Em tempos, essa forma de provar os factos era muito apoiada na prova testemunhal...”	3a
	“Em primeiro lugar, deve ter perfeito conhecimento da lei, nomeadamente a lei do cibercrime e também o CPP, para que não haja aí qualquer vício.”	3b
	“... as pesquisas têm requisitos apertados, no que diz respeito àquelas que podem ser feitas sem prévia autorização da AJ. Quanto à apreensão de dados, também há questões delicadas, e a GNR, a PSP e os demais OPC devem estar capacitados para saber aquilo que podem fazer e aquilo que exige a intervenção da AJ ou até do JIC, nomeadamente com dados que respeitem à vida íntima ou conteúdo de comunicações - por exemplo, mensagens de correio eletrónico.”	3b
	“... as medidas cautelares e de polícia, revestem aqui especial importância. No momento em que é apresentada uma queixa, quer se trate de um crime da competência da GNR ou não, é necessário que esteja preparada e consciente para, de imediato fazer a preservação da prova.”	3c
E3	“Não, porque não estão criados os sistemas e as salvaguardas que deveriam estar criados.”	3d
E4	“O regime de apreensão dos dispositivos eletrónicos, dados informáticos, correio eletrónico e registos de comunicações estão previstos nos arts. 16º e 17º da Lei do Cibercrime ...”	3b
	“... a GNR através da sua vertente de IC-Criminalística aplica em todos os processos que intervém, as melhores práticas emanadas pelo IACIS (...) para além de respeitar, como não poderia deixar de ser, as normas legais em vigor, contribuindo desta forma para a validação da prova.”	3e
E5	“... não temos recorrido a esse tipo de prova. Mas do que sei, não temos sido a força que mais tem contribuído para a apreensão de dispositivos eletrónicos.”	3a
	“Quanto ao conhecimento das normas processuais que dizem respeito à pesquisa e apreensão de dispositivos eletrónicos, presentes na Lei do Cibercrime, o comum militar da GNR que está no atendimento ainda não tem o conhecimento suficiente sobre as mesmas.”	3b 3d
E6	“No CTer Coimbra estamos a trabalhar muito bem nesse sentido, pela grande confiança que há no contacto com o MP e com o JIC. A título de exemplo, chega-nos habitualmente o material informático com o despacho do JIC para fazer a custódia da prova – recolha, selagem e envio para validação – e neste momento já temos <i>software</i> e licenciamento próprios para o fazer.”	3e

Resposta à Q4 Considera que as qualificações da estrutura de IC da GNR se encontram ajustadas à obtenção de PD?		Segmentos Identificados
E1	“O que noto na GNR é uma grande sensibilidade para o tema e vontade de desenvolver competências na área. Do contacto que tenho com Oficiais da GNR da estrutura de IC, nota-se preparação para o tema.”	4a
	“Na teoria, o que acho que deve haver é uma preparação genérica e básica sobre prova digital. (...) Como se trata de um tema muito evolutivo, é necessário fazer formação contínua, tal como fazemos no MP.”	4b
E2	“Da minha experiência, as qualificações da GNR ainda não se encontram ajustadas às especificidades da obtenção deste tipo de prova.”	4c
E3	“Do meu ponto de vista, é obrigatório que a GNR capacite toda a sua estrutura para o nível de “first response”. Desejavelmente, deve ter a capacitação de segundo grau, para exame forense, por forma a ser mais acessível a todos os CTer”	4c
E4	“Desde há quatro anos que a GNR tem, através da sua estrutura de IC-Criminalística no CTer Coimbra, um Núcleo de três especialistas a realizarem exames dentro desta temática. Recentemente foi incrementada esta valência nas instalações da Direção de Investigação Criminal em Alcabideche através da Repartição de Análise Forense Digital.”	4d
E5	“... as nossas qualificações ainda se encontram aquém daquilo que é expectável, não só naquilo que diz respeito ao conhecimento e aplicação das normas processuais penais aplicáveis à prova digital, mas também no conhecimento técnico para a sua obtenção.”	4c
E6	“... São necessários alguns ajustes de forma a evoluir nesse sentido e o NTP em Coimbra é um exemplo deste reajustar da estrutura de investigação criminal de forma a abranger também, com os devidos meios tecnológicos, esse tipo de criminalidade e de prova digital.”	4d
	“A IC tem vários cursos que são dados na EG e nomeadamente nos cursos/módulos de Análise e Informação Criminal e de Investigação Criminal o tema da prova digital já vai sendo debatido. Futuramente introduzir-se-á um módulo de prova digital, provavelmente na parte da criminalística e no curso de Investigadores.”	4e

Resposta à Q5		Segmentos Identificados
Considera que aos investigadores da GNR tem chegado conhecimento suficiente de novos métodos de investigação e de obtenção de PD?		
E1	-	-
E2	“Trata-se de uma dificuldade de todos. Até para o Ministério Público é uma luta diária e é muito difícil fazê-lo.”	5a
E3	“Aqui em Aveiro, posso dizer que sim. (...). No âmbito da passagem de informação, tento manter, dentro do possível, toda a gente atualizada.”	5b
	“Essa capacitação tem que ser feita internamente, daí a importância de criar esta estrutura de aquisição de prova a nível nacional na GNR. “	5c
E4	<p>“Uma das características do pessoal que desempenha tais funções e por inerência às mesmas é a de pesquisa contínua de novos métodos de análise e extração de dados do vestígio tecnológico que tem à sua frente.</p> <p>Diariamente saem para o mercado produtos novos, tecnologicamente mais avançados e com novas formas de segurança, proteção e defesa dos seus utilizadores.</p> <p>É imperioso que esse conhecimento chegue aos examinadores, porque doutra forma a informação que determinado vestígio contem, é inalcançável.”</p>	5d
E5	“De um modo geral, não falando apenas dos crimes cometidos através de meios informáticos ou das redes de comunicação, temos que nos adaptar sempre ao modo de atuação dos criminosos. A grande dificuldade da GNR é a velocidade de adaptação, mas, mesmo que lentamente, vamo-nos adaptando a novas formas de cometimento de ilícitos, adaptando e orientado a nossa investigação.”	5a 5e
E6	“Sim, na medida em que são utilizados pelos investigadores, e o trabalho desenvolvido pelo CTer Coimbra tem mesmo sido reconhecido por parte dos tribunais e do MP. (...) Noutros locais como Lisboa já está a haver a reformulação e investimento nesta área.”	5b 5c 5e

Resposta à Q6		Segmentos Identificados
Aquando da necessidade da realização de exames forenses para obtenção de PD, já contou com o apoio dos laboratórios da GNR? Esse contributo foi dado de forma eficaz?		
E1	-	-
E2	-	-
E3	“Pese embora com as naturais dificuldades que existem, porque é uma experiência embrionária. Há duas dificuldades que são óbvias: não se faz verdadeiramente, na maior parte dos casos, uma real pesquisa informática; tem de se melhorar a forma de apresentação dos dados.”	6a
E4	“Quanto à eficácia do trabalho dos técnicos examinadores da estrutura IC-Criminalística da GNR, os resultados falam por si, sendo elevada a taxa de condenações nos processos ondem intervém através da análise de vestígios tecnológicos e recolha de prova digital.”	6b
E5	“Tenho ouvido muitos elogios do trabalho do NTP de Coimbra, e isto é muito importante porque a PJ tem dificuldades em dar resposta a todas as solicitações que tem neste âmbito.” “Este tipo de prova requer uma resposta oportuna, e se o sistema não tiver capacidade de dar resposta em tempo oportuno, quem perde são os processos criminais e, em última instância, as vítimas. Como tal, é importante que uma força como a GNR também tenha estas valências. Com a recente criação de uma estrutura semelhante em Lisboa, conseguiremos dar ainda mais capacidade de resposta, nomeadamente na zona da Grande Lisboa.”	6b 6c
E6	“Sim, na medida em que são utilizados pelos investigadores, e o trabalho desenvolvido pelo CTer Coimbra tem mesmo sido reconhecido por parte dos tribunais e do MP.”	6b

Resposta à Q7		Segmentos Identificados
Considera que os relatórios de resultados das provas (âmbito da PD), elaborados pelos investigadores da GNR, contribuem de forma eficaz para a validação das provas?		
E1	-	-
E2	“... os relatórios que observei, encontravam-se bem elaborados, contribuindo assim para a finalidade da prova.”	7a
E3	“A apresentação dos dados é importantíssima. Os relatórios devem ser, tanto quanto possível, digitais. Aliás, a prova digital deve ser tratada digitalmente. Hoje em dia, qualquer programa utilizado para fazer recolha de prova digital permite a construção de relatórios, quer em PDF, quer em HTML.”	7b
E4	“Tem sido várias as comarcas a nível nacional a enaltecerem, a organização que damos aos processos. (...) considero que efetivamente os nossos relatórios contribuem significativamente para a validação das provas.”	7a
E5	-	-
E6	“... estamos a melhorar e que a prova digital terá grande representatividade ...”	7a

Resposta à Q8 Quais as principais lacunas/ prioridades da GNR para a obtenção de PD?		Segmentos Identificados
E1	“A falta de formação nesta área é a grande lacuna que posso apontar.”	8a
E2	“Não ter militares capacitados em todos os destacamentos para essa mesma obtenção. A falta de formação é crucial para que se possa evoluir nesse sentido.”	8a 8b
E3	“Capacitar toda a estrutura de IC com competências e conhecimento para o nível de first response, dotando todos os CTer de equipas móveis.”	8b
	“Desejavelmente ter a possibilidade de criar estruturas de segundo nível, de exame forenses, criadas nos CTer, ou pelo menos nos mais relevantes.”	8c
	“Ainda mais fundamental, é nunca parar o esforço de formação e isto está a ser feito aqui na comarca de Aveiro.”	8a
	“Há também falta de dotação de equipamentos compatíveis e de conhecimento técnico para se poder fazer a recolha de prova digital.”	8d
E4	“A falta de formação reconhecida e certificada é talvez a maior lacuna que existe neste momento. Começam a ser cada vez mais solicitadas as certificações dos técnicos par a função forense digital.”	8a
	“Além disso há que investir no parque informático, novas ferramentas, formação, equipamentos de particularidades imprescindíveis a este contexto.”	8d
E5	“Não temos ainda difundidas normas e procedimentos.”	8e
	“Existe também um desconhecimento das capacidades da estrutura criminalística da GNR, em virtude da informação não se difundir.”	8f
	“Também somos deficitários na formação dos investigadores, o curso de investigação criminal deveria ser mais objetivo, o que permitiria também abordar este tipo de temas.”	8b
	“Há falta de uma estratégia definida, para que as nossas valências não surjam de individualidades.”	8g
	“É necessário que os militares de primeira linha, nomeadamente dos PTer, estejam sensibilizados para, quando necessário, providenciarem a prova digital no âmbito das medidas cautelares e de polícia.”	8a
	“Há também necessidade de averiguar junto da magistratura quais são as necessidades que surgem, em sede de inquérito, para conseguirem produzir prova.”	8h
E6	“Formação”	8a
	“Meios/equipamentos”	8d
	“... sendo indispensável o conhecimento de toda a estrutura da investigação criminal e mesmo o MP deve estar a par das capacidades da GNR, para que os recursos disponíveis sejam corretamente utilizados e os investigadores estejam capacitados a operar no âmbito prova digital com todas as suas potencialidades.”	8f 8h

APÊNDICE H – Transcrição entrevista NTP Coimbra

Entrevistador: Miguel Ângelo Trindade Mateus

Bloco A: Caraterização do entrevistado

Nome: Rodrigues

Posto/Equivalente: Cabo

Cargo/Função: Técnico do NTP Coimbra

Unidade: CTer Coimbra

Local: Coimbra

Data: 16-05-2016

Bloco B: Guião de perguntas

1. Descreva as capacidades do NTP Coimbra para a realização de exames?

Temos capacidade para fazer exames forenses a equipamentos móveis (telemóveis e smartphones), computadores, tablets, GPS e qualquer tipo de dispositivos de armazenamento de dados.

No âmbito dos dispositivos móveis, temos duas ferramentas de análise forense – “Access Data Mobile Phone Examiner” e “UFED 4PC”.

Nos exames forenses, é possível fazer a extração de informação de 3 formas: extração física, por sistema de ficheiros e por extração lógica.

A extração física permite recuperar ficheiros apagados e permite também ultrapassar seguranças, é o tipo de extração que deve ser privilegiada. Existem dois tipos de extração física: através de “*boot loader*”, em que entramos no dispositivo pela sua raiz, pelo sistema operativo e, normalmente é por esta via que se consegue mais informação; e por ADB (Android Debug Bridge), é como se estivéssemos a aceder a uma porta de um computador tal como uma porta USB (a título de comparação).

Na extração por sistema de ficheiros poderá obter-se ficheiros apagados mas já não conseguimos fazer uma pesquisa tão profunda e também não é possível ultrapassar seguranças.

Na extração lógica, temos acesso apenas aos ficheiros disponíveis para o utilizador no sistema e não é possível ultrapassar seguranças.

O programa “UFED 4PC” permite também o exame a equipamentos GPS.

No âmbito dos GPS é também possível fazer extrações físicas. Normalmente obtemos dados sobre as localizações onde o portador do GPS esteve ou onde o equipamento foi ativado.

No âmbito dos computadores, tablets, dispositivos armazenamento e outros temos também dois programas de análise forense, sendo eles o “Belkasoft Evidence Center” e o “Access Data FTK”.

Geralmente recebemos os computadores desligados. O que fazemos é retirar o disco, ligamos aos nossos computadores através de umas portas especiais – os bloqueadores de dados – e a partir daí são extraídos todos os dados. Normalmente, apenas não temos capacidade para extrair dados que estejam encriptados. O bloqueador serve para restringir a escrita. Se nos ligarmos ao disco a partir de uma porta normal, a partir do momento em que nós entramos no disco rígido podemos fazer alterações aos dados, através desse bloqueador podemos aceder à informação sem a alterar pois ele tem a função de não permitir a escrita, apenas vamos ler os dados. É uma ferramenta que assegura que não haja corrupção nas provas.

Ao nível das buscas, trabalhamos na questão da apreensão de dados online. Ou seja, deslocamo-nos aos destinos que são alvo de busca e não apreendemos fisicamente os servidores. Esses servidores são alvo de buscas online. Ou seja, no local temos de saber quais são os dados que se pretende apreender, e fazemos a apreensão sob a forma de cópia dos dados para CD’s ou DVD’s. Neste âmbito também trabalhamos com software específico como o “X Ways Forensics” e o “OS Triage”.

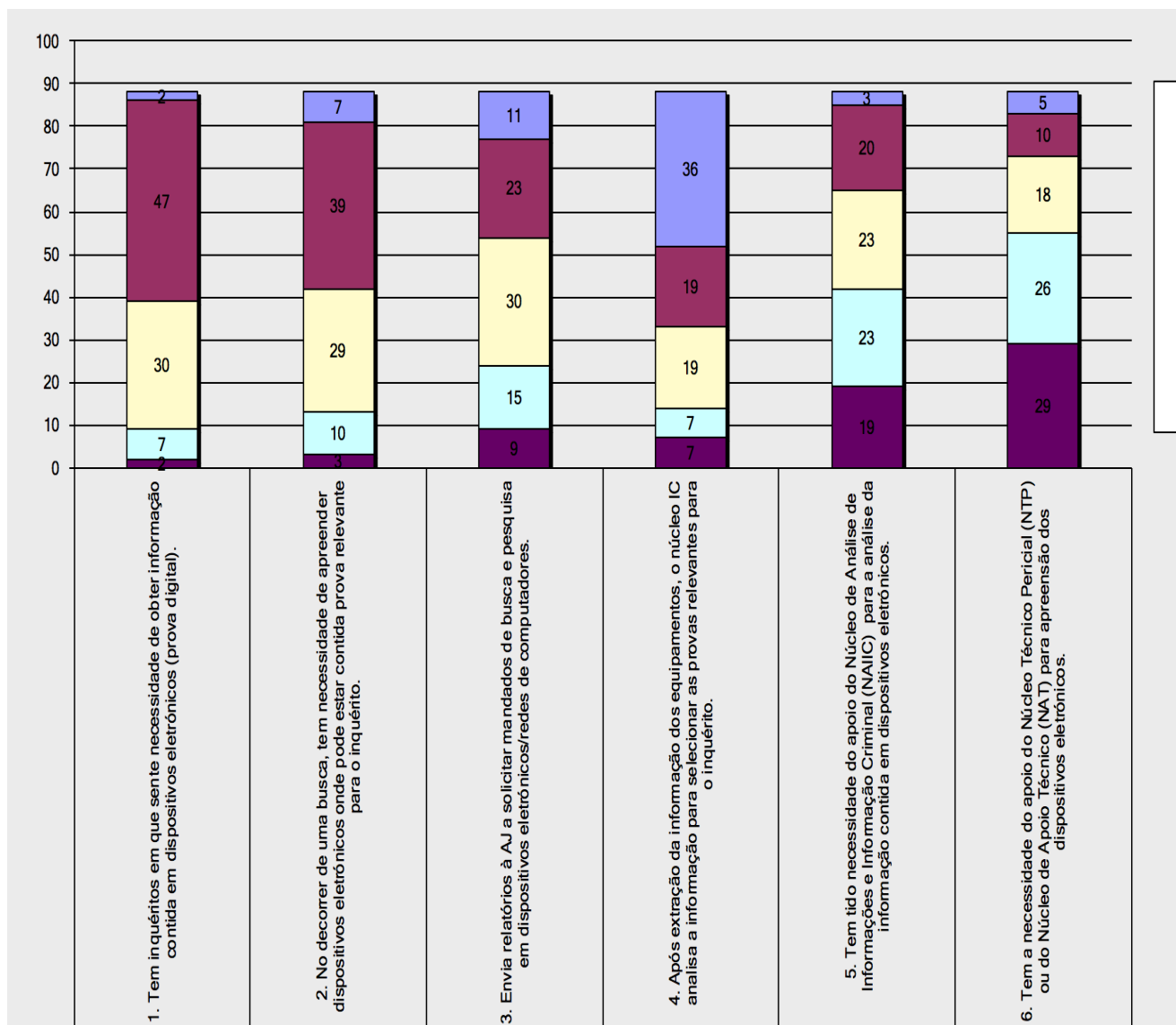
2. Quais as principais dificuldades do NTP Coimbra para o cumprimento da sua missão?

As nossas maiores dificuldades são a nível de equipamento. Neste momento estamos a trabalhar com computadores que não são os ideais, tratam-se dos mesmos computadores que, por exemplo, uma secretaria usa. Deveríamos ter computadores mais sofisticados. Felizmente, na repartição que abriu em Lisboa, já estão capacitados com computadores mais sofisticados e adequados para o desempenho deste tipo de atividade.

3. Em média, quais os tempos de espera para a exportação dos exames pedidos?

Em 2015, conseguimos dar uma resposta, sensivelmente, até dois meses. Este ano os exames estão a aumentar e esse período de resposta é superior, visto que já fizemos cerca de 517 exames e temos mais de 600 pendentes.

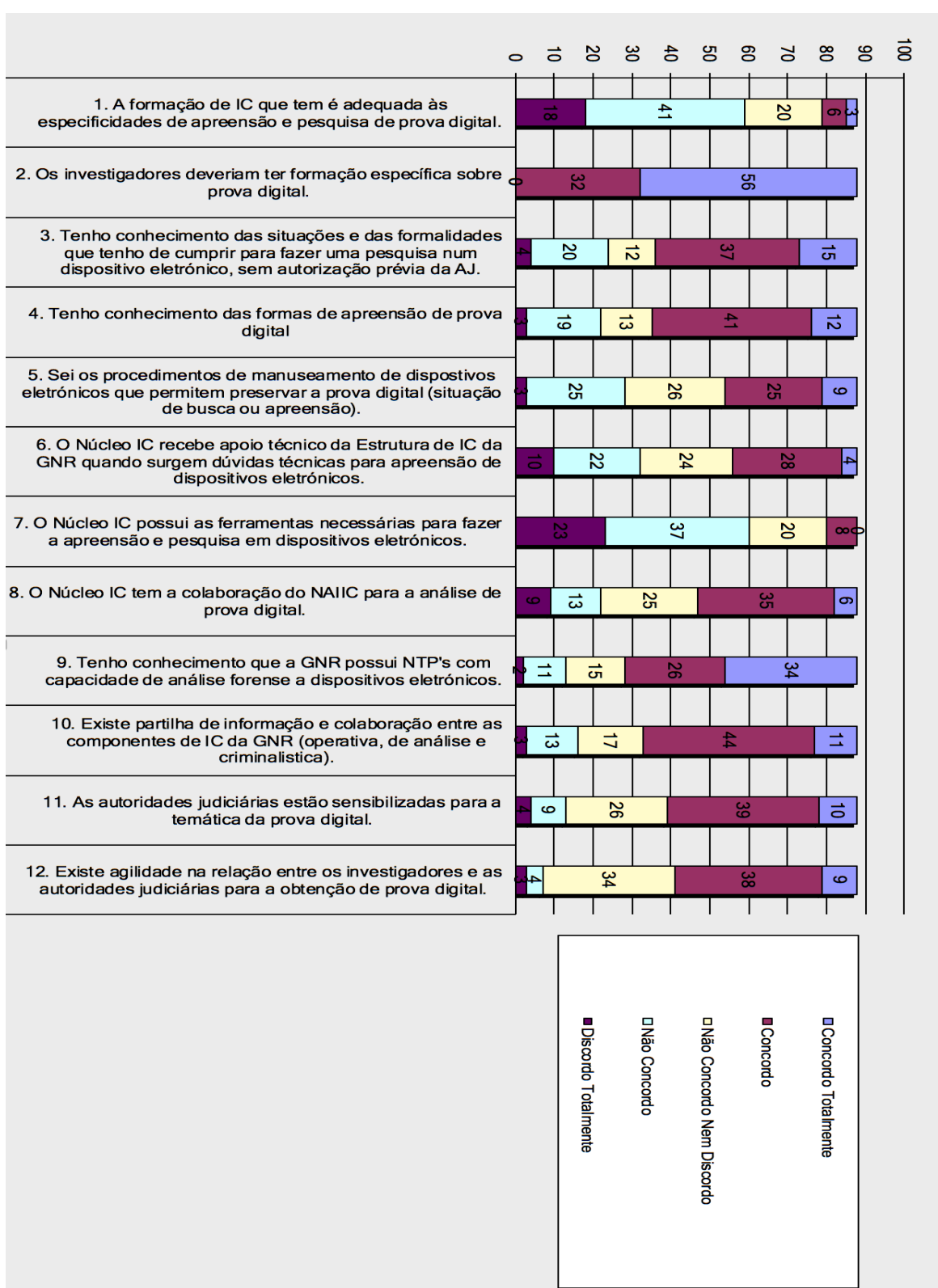
APÊNDICE I – Respostas à questão 1 do grupo 3 do questionário



Fonte: Elaboração própria.

APÊNDICE J – Respostas à questão 2 do grupo 3 do questionário

Apêndices



Fonte: Elaboração própria.