INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Dissertação de Mestrado em Ciências Policiais

Área de especialização em Gestão da Segurança

Perícia Digital Forense em Portugal:

O caso da exploração sexual de menores no Ciberespaço

Orientação científica:

Orientador: Professor Doutor Sérgio Ricardo Costa Chagas Felgueiras

Superintendente da Polícia de Segurança Pública

Coorientador: Mestre António Lourenço Gomes Pimentel

Subintendente da Polícia de Segurança Pública

Margarida Nunes Carvalho

Abril, 2024

Agradecimentos

Concluída mais uma etapa do meu percurso académico, chega o momento de agradecer a todos aqueles que marcaram esta minha jornada e contribuíram para a realização desta dissertação.

Primeiramente, ao Instituto Superior de Ciências Policiais e Segurança Interna pelo prestigiado quadro docente que proporciona um ensino de referência na esfera das Ciências Policiais. Ao sítio onde mergulhei na área que hoje é paixão, espero um dia cá regressar.

Ao Departamento de Investigação Criminal, nomeadamente o Laboratório de Criminalística e Ciência Forense, que durante meio ano foi segunda casa e me fez vestir o *amor à camisola.*

Ao meu orientador Professor Doutor Sérgio Ricardo Costa Chagas Felgueiras, Superintendente da Polícia de Segurança Pública, académico e professor de excelência, com quem tive a honra e privilégio de trabalhar e aprender sempre um pouco mais. À pessoa que confiou no meu trabalho, um enorme obrigada.

Ao meu coorientador Mestre António Lourenço Gomes Pimentel, que permitiu que o estágio se concretizasse, demonstrando inteira disponibilidade para acompanhar e responder a qualquer adversidade que surgisse.

Ao Chefe Gonçalves, que me orientou incansavelmente durante todo o estágio, a quem estou eternamente grata por me fazer sentir bem-vinda dia após dia. Aos meus camaradas Agente-Principal Lourenço, Agente-Principal Cabral e Agente-Principal Rodrigues por todo o tempo despendido dando-me a conhecer a realidade policial. Para além de profissionais foram também confidentes e aliados das minhas pequenas conquistas.

Às minhas amigas, que levarei comigo para a vida, que foram os ouvidos das minhas frustrações, a companhia dos meus dias de escrita, o conselho prudente durante este percurso. A leveza nos momentos mais pesados. Ao André, que me fez crescer enquanto pessoa e acreditou em mim, mesmo quando eu não o fazia.

Aos meus pais, as pessoas mais importantes da minha vida, que são, sempre foram e sempre serão meus pilares na caminhada da vida. Aqueles que permitiram que tudo isto se concretizasse e me educaram com os ingredientes necessários para ser a jovem mulher que hoje sou.

À minha avó Teresinha que me demonstrou que é na dificuldade que se vê a força e, por fim, ao meu avô e à Mulher com “M grande” que farei por me tornar, como um dia lhe prometi.

Resumo

O Ciberespaço possui duas faces que se distinguem: por meio da visão utópica traduz-se numa ferramenta fundamental na mitigação e prevenção da criminalidade, outrora, soma-se a ela uma personalidade obscura, permeável a qualquer indivíduo carregado de intenções maliciosas, ou seja, é também ele uma ameaça em si (visão distópica). Assim, não só emerge uma nova forma de crime - crime informático - como o crime tradicional é também convidado a desenvolver-se nesta nova forma de espaço. Por conseguinte, a fusão do crime com o digital faz da prova digital um valioso meio de auxílio à investigação criminal na condenação daqueles que se dedicam a tais práticas criminosas. Na presente investigação, a exploração sexual de menores no Ciberespaço, uma e-ameaça crescente e reticular, é desenhada como um fenómeno que necessita de devida atenção na sua vertente legal, policial e académica (teórica, empírica e normativa).

Palavras-chave: ciberespaço; e-ameaça; exploração sexual de menores; perícia digital forense; prova digital.

Abstract

We may say cyberspace has two distinct sides: through the utopian vision, it becomes a fundamental tool for mitigating and preventing crime, while on the other hand, it has a dark personality, permeable to any individual with malicious intentions, which it's also a threat itself (dystopian vision). So, not only does a new form of crime emerge (cybercrime), but the traditional crime is also invited to develop in this new form of space. Therefore, the fusion of crime and the digital makes Digital Evidence a valuable way of supporting criminal investigation in convicting those who engage in such criminal practices. In this paper, the sexual exploitation of children in cyberspace, a growing and widespread e-threat, is described as a phenomenon that needs due attention in its legal, police and academic aspects (theoretical, empirical and normative).

Key-words: cyberspace; e-threat; children sexual exploitation; digital forensics; digital evidence.

Índice

Índice de Tabelas

Índice de Figuras

Índice de abreviaturas, siglas e acrónimos

Art.	Artigo
CDC	Convenção das Nações Unidas sobre os Direitos da Criança
EMGFA	Estado-Maior-General das Forças Armadas
ESM	Exploração Sexual de Menores
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
FSS	Forças e Serviços de Segurança
IC	Investigação Criminal
MDN	Ministério da Defesa Nacional
MP	Ministério Público
NATO	*North Atlantic Treaty Organization*
OPC	Órgãos de Polícia Criminal
PSP	Polícia de Segurança Pública
PJ	Polícia Judiciária
TC	Tribunal Constitucional
TIC	Tecnologias da Informação e Comunicação
UE	União Europeia

Introdução

A sociedade contemporânea é crescentemente dinâmica, globalizada e tecnológica, marcada pela complexidade de novos riscos e ameaças, também eles progressivamente flexíveis. Atualmente, várias formas de crime migram para o Ciberespaço, sendo o meio informático um auxílio recorrente para concretização de uma ação criminosa independentemente da sua tipologia. Tem-se igualmente presente que as menores e os mais jovens sentem enorme atratividade pelas novas tecnologias que, dissociados dos perigos a elas inerentes, se expõem a um problema alarmante: a exploração sexual de menores no Ciberespaço. No contexto do século XXI, esta forma de crime é enquadrada como uma nova ameaça alvo de preocupação da comunidade internacional face ao seu crescente aumento, que acompanha o ritmo acelerado da digitalização. A exploração sexual de menores no Ciberespaço desfila como parte de "[...]fenómenos securitários cada vez mais intrincados e desafiadores numa sociedade do risco, da incerteza e da imprevisibilidade" (Elias, 2018, p. 33) sendo fundamental a problematização desta realidade.

E é a necessidade de problematizar o cenário securitário, na procura de respostas a fenómenos cada vez mais desafiantes, que conduziram à emergência das Ciências Policiais. Estas Ciências aplicadas podem entender-se como "o estudo da produção da segurança pela polícia" (Clemente, 2015, p. 16) e procuram desenvolver a investigação multidisciplinar em áreas basilares para a segurança, onde se insere o estudo para prevenção e combate aos vários riscos e ameaças existentes. É neste contexto que surge a pertinência desta dissertação no Mestrado em Ciências Policiais com especialização em Gestão da Segurança, que incide sobre as técnicas e procedimentos utilizados pela ciência forense digital, em Portugal, na aquisição e valoração da prova digital no que concerne à exploração sexual de menores num espaço que teima em não parar de mudar - o Ciberespaço. Exige-se uma constante adaptação das forças e serviços de segurança na mitigação desta forma de ameaça, que se inicia na consciencialização sobre o que enfrentamos e no estudo da matriz de resposta atual.

Na revisão literária efetuada foi possível constatar que, em Portugal, o crime de abuso sexual de menores é bastante explorado nas suas mais variadas vertentes, caminhando entre as áreas da psicologia, direito, ciência forense, investigação criminal, entre outras. Outrora, quando a ele se soma o domínio do Ciberespaço, a literatura é escassa face ao expectável. No entanto, desta pequena parcela de bibliografia sobre o tema, foi encontrada uma dissertação de

Mestrado intitulada de “A Exploração Sexual de Menores no Ciberespaço - aquisição e valoração de prova forense de natureza digital” de Magriço (2012), adaptada em livro no ano de 2014.

Curioso como, desde então, os três temas que abrangem - Ciberespaço, exploração sexual de menores e prova digital - têm vindo a ser imensamente explorados individualmente, mas conjugados compõe um vazio bibliográfico. Eis que, passados mais de 12 anos desde a análise realizada por Magriço (2012), surgiu a vontade de responder à questão de partida e algumas questões derivadas como forma de dar resposta a esta lacuna, sobre um desafio que apesar de discutido há uma década, é tão atual e tenderá a assumir uma ameaça de elevado grau nos próximos anos. Apesar de uma abordagem distinta, importa perceber em que medida evoluiu esta problemática, bem como é atualmente realizada a aquisição e valoração da prova digital deste tipo de atividade criminosa.

Assim, tem-se como problema de investigação: “Tendo em consideração a transferência para o Ciberespaço de atividade delituosa relativa à exploração sexual de menores (ESM) é possível implementar procedimentos de Investigação Criminal (IC) que, com eficácia, acautelem a aquisição de prova digital e potenciem a condenação dos que se dedicam a tais práticas criminosas?” Tendo em conta que se trata de uma investigação que aborda a recolha de “prova digital” nos casos “exploração sexual de menores” no “Ciberespaço”, é fulcral questionarmos sobre cada um destes pontos, individualmente. Para prova digital, é necessário perceber em que medida evoluiu o regime jurídico da prova digital na última década (partindo da análise de Magriço (2012), se são seguidos procedimentos e metodologias de investigação padrão para recolha de prova digital nos casos de ESM *online*. Para exploração sexual de menores, questionar se o quadro normativo português responde corretamente às necessidades exigidas por este tipo de atividade criminal, e em que medida deverão os nossos OPC de competência genérica ser dotados de maiores competências de IC, nesta matéria. Na dimensão do Ciberespaço, compreender quais as restrições por ele impostas às investigações nos casos de exploração sexual de menores. A necessidade de problematização destes pontos advém da correlação indireta com a pergunta de investigação a que nos propomos a responder.

Como tal, também no seu desenvolvimento pretendemos responder a questões como:

- Como evoluiu o regime jurídico da prova digital, na última década?
- A nível nacional são seguidos procedimentos e metodologias de investigação padrão, neste âmbito?
- Na dimensão do Ciberespaço, quais as restrições às investigações nos casos de exploração sexual de menores?

- Estará a lei portuguesa em conformidade com as necessidades exigidas por este tipo de atividade criminal?
- Deveremos dotar os nossos OPC de competência genérica de maiores competências de IC, nesta matéria?

Com o intuito de responder à pergunta de partida e restantes questões acima colocadas, considerámos pertinente dividi-la em quatro grandes momentos. Primeiramente, pretendeu dar-se uma contextualização sobre a sociedade de informação e o surgimento do Ciberespaço, devidamente concetualizado e demarcado na sua dimensão geográfica - porque assume um carácter global e transcendente - e securitária - porque, para o efeito, importa vê-lo como um espaço para onde o crime é convidado. De seguida, abordaremos a forma de crime em análise - a exploração sexual de menores, limitada ao Ciberespaço - como uma e-ameaça em crescimento, a personalidade pela qual é revestida e os instrumentos jurídicos nacionais e internacionais que pretendem responder a esta problemática. Ressalva-se que não é um objetivo explorar esta forma de crime aprofundadamente. Já num terceiro momento dissertaremos sobre a esfera da prova digital, na qual se insere o estudo sobre a sua natureza jurídica, a cadeia de custódia da prova, os métodos, procedimentos e recomendações de boas práticas para uma correta preservação da prova.

E para uma análise devidamente sustentada sobre o tema, a componente prática foi considerada essencial. Como tal, e com o objetivo de conferir robustez ao trabalho, no último capítulo (capítulo 4) será desenvolvido um caso que simula um episódio de exploração sexual de menores no Ciberespaço sobre o qual serão aplicadas técnicas e procedimentos forenses utilizados pela Polícia de Segurança Pública (PSP) na realização de uma perícia informática e, por conseguinte, produção de prova. A simulação desta investigação criminal decorre de um estágio curricular que ocorreu no Departamento de Investigação Criminal da PSP, em Belas, Lisboa, por um período de 6 meses, cuja autorização consta no Anexo F.

Por outro lado, a elaboração da presente dissertação tem também como primordial objetivo servir de apoio e contributo a projetos e estudos que trabalhem questões do digital forense, distinguindo-se dos demais ao abrir portas ao trabalho realizado por um Órgão de Polícia Criminal português - Polícia de Segurança Pública - na execução de uma perícia digital forense ao ano de 2023/2024.

E apesar de, hoje, a exploração sexual de menores no Ciberespaço não representar uma prioridade para as forças e serviços de segurança nacionais quando comparada a outros crimes com maior expressão em Portugal (caso da violência doméstica, tráfico de estupefacientes, por

exemplo), é facto que esta é uma realidade em crescendo que tende a acompanhar a evolução da internet. Assim, a elaboração da presente dissertação representa igualmente um exercício de prospetiva que, sem a devida prevenção e adequação das nossas forças policiais, poderá representar uma ameaça de grande peso e em larga escala, naquele que se desenha como um futuro incerto.

Método

No desenvolvimento da presente dissertação, optámos por realizar um estudo exploratório, considerando a investigação limitada sobre a presente área temática, procurámos ler e analisar a bibliografia disponível sobre o tema, com o objetivo de compreender e descrever o objeto de estudo – a recolha de prova digital nos casos de exploração sexual de menores no Ciberespaço. Com recurso a uma abordagem qualitativa, pretendeu-se recolher e tratar informação considerada relevante para, posteriormente, formular uma análise crítica devidamente sustentada. Para melhor organizar e sintetizar as ideias, foram preenchidas fichas de leitura organizadas categorialmente para viabilizar a simplificação, o tratamento e a análise da informação.

O objeto de estudo pode ser caraterizado pela interseção das três áreas temáticas supramencionadas, designadamente, o Ciberespaço, a prova digital e a atividade criminosa de ESM. Objetivamente, para o enquadramento da investigação, realizou-se uma extensa revisão bibliográfica alicerçada na consulta dos principais autores que se debruçam sobre o tema da sociedade de informação e o Ciberespaço, nomeadamente Bell (1976), Gibson (1984) e Castells (1996), a par da análise de dados que permitam a quantificação do problema e a sua expressão global/europeia, estes foram expostos como forma de melhor percecionar esta realidade, enquanto uma ameaça à segurança. Destaca-se, para o efeito, o *Digital Global Overview Report* (2023), um dos principais relatórios sobre o mundo digital que alia várias organizações internacionais de referência.

Seguidamente, ao introduzir a exploração sexual de menores no Ciberespaço, procedeu-se à consulta de legislação nacional e europeia, bem como dos principais relatórios que mencionam este tema como uma ameaça a combater (por *e. g.* Constituição da República Portuguesa (CRP), Convenção sobre os Direitos das Crianças (1989), Diretiva n.º 2011/92/UE do Parlamento Europeu e do Conselho de 13 de Dezembro de 2011, Código Penal, *Spotlight Report on Child Sexual Exploitation* (2023), Estratégia da UE para uma luta mais eficaz contra o abuso sexual das crianças (2020), Estratégia europeia para uma Internet melhor para as crianças (2012), Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas (EMPACT), *Internet Organised Crime Assessment* (IOCTA) (2023) e Relatório Anual de Segurança Interna (2022).

Depois de contextualizado o crime e o espaço onde ele ocorre, o foco da investigação foi então introduzida, sendo para tal examinados concretamente a ISO 27037, de 2012 - documento internacional - e o Manual Técnico de Preservação e Recolha da Prova digital na

Investigação Criminal da PSP (2015) - documento nacional - sem descurar do Código Processual Penal, Lei do Cibercrime, entre outros, com o intuito de descrever os procedimentos e técnicas utilizadas em Portugal para a preservação do local e constituição de prova digital.

Posteriormente, imergimos no exercício prático da dissertação. Sendo que a ciência se inicia com a observação e formulação de um problema (Santos, 1994), a técnica da observação foi um dos métodos utilizados para realização da simulação de investigação, fulcral para adquirir informações sobre um fenómeno, evento ou objeto de estudo.

Para elaboração da mesma foram utilizados *hardwares* e *softwares* forenses em uso da Polícia de Segurança Pública no Setor Digital Forense (*Cellebrite UFED Touch 2, Cellebrite Physical Analyzer*, *OpenText EnCase Forensics e o Tableau TD3*), em três sistemas informáticos (Iphone 7, Samsung Galaxy S8, Toshiba NB305-10G), simulando um caso de ESM para uma posterior análise e discussão de resultados com base no método referido. Todas as técnicas de recolha de prova aplicadas foram cuidadosamente assistidas por peritos informáticos forenses da PSP para uma simulação o mais idêntica à realidade quanto possível. Os métodos, materiais, e procedimentos utilizados para elaboração do mesmo foram detalhadamente descritos no capítulo 4.

Em suma, para uma melhor compreensão do estudo de caso foi fulcral a definição de conceitos operacionais que estarão presentes ao longo do trabalho de investigação, tornando-se estruturantes do mesmo. Deles destaco os conceitos de Ciberespaço; e-ameaça; exploração sexual de menores; prova digital e perícia digital forense.

Capítulo 1 – O Ciberespaço: enquadramento temático e concetual

1.1. A ascensão da Era Informacional

Iniciamos este capítulo com recurso a uma metáfora utilizada por Toffler (1980) que sugere que o mundo, fruto da evolução, tem sido inquestionavelmente moldado por três ondas de inovação tecnológica, que revolucionaram não só toda a estrutura social, mas também o modo como o Homem nela se posiciona. A primeira referente à Revolução Agrícola (processo gradual que ocorreu ao longo do século XVIII) precedida pela Revolução Industrial (que se alastrou pela Europa no decurso do século XIX) e, finalmente, a Revolução da Informação[1] que, para além de conhecida por todos nós, é também vivenciada desde o século XX. O ponto de partida da presente investigação visará sobre este último ponto, explorada de forma aprofundada neste capítulo.

A evolução das diversas formas de transmitir informação tem moldado a sociedade contemporânea a um ritmo alarmante, que não parece contestar o novo rótulo que se impõe. Fruto de toda uma conjuntura histórica, social e económica, assistimos a um processo constante de inovação que desempenha um papel determinante na criação de produtos e serviços que originam novas formas e estilos de vida. Em sentido figurado, Dijk (2006) descreve que, na atualidade, se constroem estradas e pontes a uma velocidade difícil de acompanhar - "Estas estradas são destinadas à informação e comunicação" (p. 1) - que, aparentemente, são parte de uma realidade abstrata e compõe a chamada sociedade informacional (ou Era da informação) que assenta na informação e nas tecnologias da informação e da comunicação (TIC). Todos os dias recebemos e geramos informação em tempo real, originando-se um ciclo de troca de informação que se materializa, na sua grande maioria, com recurso às novas tecnologias: representam novas formas de nos relacionarmos enquanto comunidade, revolucionando toda a interação humana e exercendo influência, de forma significativa, nos mais diversos setores. Por outras palavras, nesta sociedade, a informação traduz-se num estímulo de crescimento económico, social, político e cultural que se promove por via das redes e se faz notar de forma incontestável.

Toda esta conjuntura culminou numa inovação sem precedentes. Posto isto, dá-se o nome de revolução da informação, em curso desde as décadas de 60 e 70 do século XX, a todas as alterações provocadas pelos avanços das TIC e que simboliza, de facto, a ascendência da

[1] Do inglês, *information revolution*.

cultura do digital ou, como é correntemente denominada, sociedade da informação (Castells, 1996).

A noção de sociedade de informação tem sido alvo de debate entre diversos autores que trabalham no sentido de encontrar uma definição que melhor traduza o seu significado. Webster (2002) defende que é possível explicar a sociedade da informação de múltiplas formas consoante a ótica pela qual é analisada: perspetiva tecnológica, espacial, ocupacional, cultural e económica. Apresenta-se de forma sucinta os diferentes ângulos.

De acordo com Webster, as novas tecnologias são um dos principais indicadores da sociedade contemporânea, que anunciam a chegada de uma sociedade de informação, "vozes que se fazem ouvir anunciam que uma nova ordem…se enaltece num mundo desprevenido" (2002, p.10) como resultado dos avanços nas telecomunicações. Ou seja, não estamos apenas ligados por estradas, cabos elétricos, caixas de correio e televisões por cabo, mas também a redes informáticas como a internet, que exponencia um novo estilo de vida assente na informação e no digital.

A segunda abordagem possível (espacial), que evidência o carácter geográfico, assenta na premissa de um mundo interligado, apesar das distâncias que nos separam - "estamos todos conectados" (Webster, 2002, p. 17) - em resultado, sobretudo, da globalização que "[…] fornece meios tecnológicos para que os transportes sejam mais baratos e as comunicações facilitadas" (Oliveira, 2017, p. 10). Num mundo que se reduz em dimensão perante o efeito das novas tecnologias da comunicação, dá-se uma redefinição do fator tempo e espaço, permitindo uma sociedade de indivíduos conexos ao nível nacional e internacional.

Profetizando a "reunificação da humanidade numa comunidade à escala global" (Guedes, 2015, p. 193), nos anos 60 do século XX, Marshall McLuhan (1964) refere-se a "aldeia global" para descrever a sociedade contemporânea, unificada graças ao advento da eletrónica e das TIC. Isto é, permitimo-nos chegar a qualquer canto do mundo, independentemente das barreiras físicas que nos separam, tendo em conta que as próprias redes expandem o seu alcance e capacidades de forma exponencial (Urry, 2000).

Outra abordagem, que encontra o seu ponto de partida no estudo de Daniel Bell (1976), é a ocupacional. Esta abordagem atenta que vivemos numa sociedade da informação tendo em conta que o "grupo predominante [de ocupações] consiste em trabalhadores da informação" (Bell, 1979, p. 183). A obra *Living on Thin Air*[2] (1999) sustenta que pensar de forma inteligente,

[2] Obra de Charles Leadbeater (1999) que evidencia a influência da informação na contemporaneidade.

ser inventivo e deter capacidade de desenvolver e explorar redes é, na verdade, a chave para a nova economia *weightless*[3] já que a produção de riqueza provém, não do esforço físico, mas de "ideias, conhecimentos, habilidades, talento e criatividade" (Leadbeater, 1999, p. 18). Esta abordagem conduz a uma conceção de sociedade de informação mais facilmente reconhecida, mas a menos medida: a cultural. Isto é, face à penetração das TIC nas sociedades, faz-se emergir um novo estilo de vida. O modo de agir, pensar, atuar, dos indivíduos altera-se; enraizou-se, tornou-se cultural, passaram a dominar as nossas vidas.

Por fim, e muito brevemente, a abordagem do ponto de vista económico, "Esta abordagem mapeia o crescimento do valor económico das atividades informativas" (Webster, 2002, p. 12).

Outrora, apesar de justificarem a mesma realidade através de diferentes óticas, nenhuma destas abordagens deve ser considerada isoladamente, funcionando sob uma relação de interdependência.

De acordo com Dijk (2006, p. 2), "Num tom de exagero, podemos chamar ao século XXI a Era das redes". Isto permite-nos avançar para um conceito interdependente quando abordamos a questão da sociedade da informação: a sociedade em rede.

A expressão *network society* nasceu de um estudo de Manuel Castells nos anos 70 do século XX que hoje representa uma sociedade na qual as relações sociais, económicas e políticas são fortemente influenciadas e mediadas pelas TIC, especialmente através da internet. Verifica-se uma tendência de evolução do sistema mediático como elo entre indivíduos e organizações, cujas relações passarão a ser progressivamente estabelecidas em ambientes multimédia e a sua relevância social dependerá da sua presença digital (Castells, 1996). Origina-se, assim, uma rede global de comunicação e interação que exige uma permanente adaptação de todos os atores sociais.

Acrescenta-se ainda que "os dispositivos tecnológicos mudaram radicalmente e substancialmente o mundo e o lugar do Homem" (Martins, 2012, p. 33). Dito isto, pode afirmar-se que, a longo prazo, a interação com computadores e outros tipos de media possa representar um fator de mudança no comportamento humano, que Dijk (2006) relata como "[…] influência dos media sobre o espírito humano" (p. 233). O autor, partindo desta premissa, agrupa vários traços individuais e divide-os em cinco tipos de personalidade que acredita que possam advir futuramente de uma experiência próxima aos novos media: personalidade rígida ou formal;

[3] Expressão do inglês. Que não necessita do uso da força.

personalidade computadorizada; personalidade antisocial; *C'borgs* e personalidade múltipla. Esta última, por exemplo, é justificada pela facilidade do utilizador em assumir uma outra identidade que não a sua, promovendo a questão da diversidade de personalidades, que varia de acordo com o contexto social em que o indivíduo se insere.

Neste sentido, tendo em conta o até então descrito, surge uma nova dimensão que liberta o Homem da presença física, permitindo-lhe conhecer uma nova forma de contacto, de amplificar a comunicação, encurtar distâncias geográficas, alterando drasticamente a forma como se relaciona em sociedade. Constata-se que, ao mundo na sua forma física, soma-se um outro elemento que incorpora toda a realidade abstrata, invisível: o Ciberespaço.

Discutir a "Era Informacional" é, portanto, fulcral para a contextualização da esfera do Ciberespaço - um dos pilares fundamentais da presente investigação - onde se movimenta a sociedade atual e por onde navega o crime sobre o qual nos propomos a dissertar.

1.2. O Ciberespaço

1.2.1 Definição concetual

No sentido de melhor percecionar o domínio do Ciberespaço, e sem intenção de apresentar definições incontestáveis e definitivas, considerámos imperiosa uma explicação sumária do conceito – ou melhor, dos vários conceitos que pretendem explicar o Ciberespaço - e para tal, recua-se à palavra que denota a sua origem: "cibernética".

A palavra cibernética, do grego *kybernētēs* – arte de governar, arte de pilotar - utilizada por Homero na Odisseia como Timoneiro, isto é, o responsável pela navegação, denuncia, desde a sua criação, a relação entre a máquina e o Homem e o seu domínio sobre a mesma. Mais tarde, a terminologia foi empregue na obra *Cybernetics: Or Control and Communication in the animal and the Machine* (1948), do matemático norte-americano Norbert Wiener, que fez uso do termo para descrever um novo campo que se centra na comunicação e no controlo de sistemas, dando origem à palavra inglesa *cybernetics*, cuja tradução para português se refere a "cibernética". Quase quatro décadas mais tarde, 1984, estreia-se a terminologia "Ciberespaço" pelo autor de ficção William Gibson (1984) nos livros *Burning Chrome* e *Neuromancer,* descrevendo-o como:

> Uma alucinação consensual experimentada diariamente por biliões de operadores legítimos, em todas as nações, por crianças a quem são ensinados conceitos de matemática... Uma representação gráfica de dados extraídos dos bancos de dados de

> cada computador no sistema humano. Complexidade impensável. Linhas de luz no espaço da mente, grupos e constelações de dados (p. 67).

Desde então, acompanhando a expansão das TIC, a palavra ultrapassou as barreiras da ficção científica e é utilizada em diversas áreas do conhecimento humano, identificada de forma proeminente como sinónimo do mundo digital. Quando nos referimos ao Ciberespaço "[…] algumas palavras podem ser naturalmente associadas, tais como computador, rede, Internet, dados e informação, *hardware* e *software*, comunicação, etc" (Ning *et al*., 2018, p. 1844), porém, a sua definição e compreensão é um assunto complexo que envolve um conjunto de ciências e, tal como qualquer outro conceito de natureza interdisciplinar, uma compreensão integral requer a consideração de diferentes perspetivas.

Ora, de acordo com John McLeod (1997), "[…] as histórias são formas de dar sentido ao mundo e ao nosso lugar nele". É sobre este ideal que Bell (2001) inicia a sua reflexão sobre o Ciberespaço, na obra *An introduction to cybercultures*. Multifacetado, de difícil definição e dependente da ótica pela qual é percebido, vivenciado, notado, é este o modo como o autor se refere ao espaço ciber, destingindo-se dos demais ao adotar um conceito construído em função do *story telling*[4], "Quero concentrar-me nas formas como se fala e escreve sobre o Ciberespaço. Irei escolher uma série de formas de contar histórias sobre o Ciberespaço, e irei explorar os tipos de histórias que têm sido contadas" (Bell, 2001, p. 6).

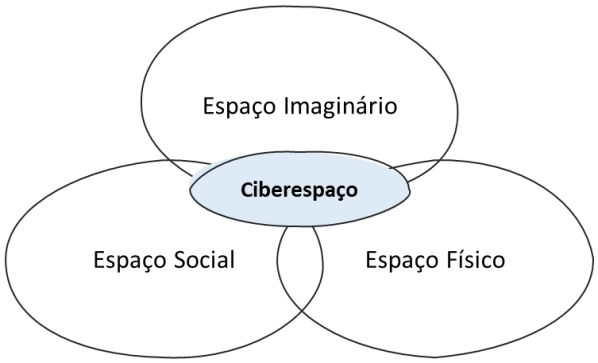
Assim, defende que existem 3 formas de percecionar o Ciberespaço: dimensão material, simbólica e experimental. Divide-o, para tal, em "what it is" – o Ciberespaço enquanto *hardware*, por exemplo, uma rede de computadores que se conectam através de infraestruturas de comunicação, que facilitam as formas de interação entre atores remotos – "what it means" – a perspetiva simbólica; um universo idílico onde o protagonista (o utilizador) poderá envolver-se numa realidade ímpar, construída e idealizada à sua medida, acrescentando ao *hardware* um espaço abstrato de imagens e ideias – e por fim, "what it does" – baseada na forma como todos experienciamos o Ciberespaço combinando a sua vertente material e simbólica.

Ning *et al*., (2018, p. 1845) argumenta que " […] ciberespaço num sentido convencional refere-se ao espaço metafórico digital, virtual, abstrato e independente do tempo, baseado em redes de computadores globalmente interligadas e a todas as infraestruturas e elementos a ele relacionados". Para melhor sustentar o seu argumento, à semelhança de Bell (2001), o autor distingue três vertentes do Ciberespaço: "O ciberespaço é o mundo digital baseado nos

[4] *Storytelling* ('story' do inglês 'história' e 'telling' referente a 'contar') consiste na atividade de comunicar através da criação de narrativas com o intuito de envolver pessoas, transmitir ideias, conceitos e produtos.

tradicionais espaços físicos, sociais e de pensamento (FSP) […]" (p. 1843). O espaço físico cibernético referente aos dispositivos e infraestruturas materiais da qual depende o seu funcionamento, ou seja, toda a estrutura material; o espaço social cibernético alusivo à instituição de normas e leis que permitem a sua regulação; e o espaço imaginário ou espaço de pensamento cibernético (*thinking space*) enquanto fonte de criação, integrante do intangível; observável na Figura 1.

Figura 1. Ciberespaço e os espaços tradicionais



Fonte: Adaptado de (Ning *et al.).*

Um novo universo - um paralelo universo - suportado pela rede global de computadores e redes de comunicação; uma série de ideias, problemáticas e questões que surgem quando conjugados o prefixo 'ciber' – "representativo das actividades electrónicas e informáticas" (Nye, 2010, p. 3), que apela ao imaginário do virtual - e a palavra 'cultura' (Bell, 2001, p. 1). Ou seja, "[...] o ciberespaço serve de molde a partir do qual um conjunto de neologismos é criado: ciberpunk, cibercultura, cibervida, cibernautas, cibersexo, cibersociedade, cibertempo - *cibertudo"* (Strate, 1999, p. 382), cunhado, portanto, por um prefixo que remete qualquer palavra ao universo do abstrato e transcendente.

Para uma compreensão *latu senso* do tema, foi feita uma revisão das mais recentes Estratégias de Cibersegurança Nacional de países como os Estados Unidos, Canadá e estados europeus, e outros documentos relevantes no domínio securitário que apresentam uma definição de Ciberespaço.

Tabela 1. Definições gerais do conceito de "Ciberespaço" em documentos oficiais

"[…] um domínio global pertencente ao ambiente informacional, que consiste na rede interdependente de infraestruturas das tecnologias da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas informáticos, e processadores e controladores incorporados". **------- Departamento de Defesa (DOD) dos Estados Unidos "Dicionário Militar e Termos Associados" 2021**
"O mundo eletrónico criado por redes interligadas de tecnologia da informação. É uma comunidade global onde mais de 3 mil milhões de pessoas estão conectadas entre si para trocar ideias, serviços e relações de amizade". **------- Canadá, "Estratégia de Cibersegurança Nacional", 2018**
"O ciberespaço é uma rede interdependente de tecnologia da informação que inclui a Internet, redes de telecomunicações, sistemas informáticos e dispositivos ligados à Internet. Para as forças armadas [...] é um domínio operacional, juntamente com a terra, o mar, o ar e o espaço". **------- Reino Unido, "Estratégia Nacional Cibernética:", 2022**
"O ciberespaço é a área virtual de todos os sistemas de tecnologia da informação do mundo, que estão ou poderiam estar interligados a dados. O ciberespaço, enquanto rede acessível pública, acede-se através da Internet, que pode ser expandida por meio de quaisquer outras redes de dados". **------- Alemanha, "Estratégia de Cibersegurança da Alemanha", 2021**
"O ciberespaço é um domínio artificial composto essencialmente por nós e redes de TIC, armazenando e processando uma riqueza cada vez maior de dados de importância estratégica para Estados, empresas e cidadãos, e para todos os decisores políticos, sociais e económicos". **------- Itália, "Quadro Estratégico Nacional para a Segurança do Ciberespaço", 2013**
"[…] ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação". **------- Portugal "Estratégia Nacional de Segurança do Ciberespaço 2019-2023"**
"Ciberespaço: o espaço de comunicação criado pela interligação mundial de infraestruturas de processamento automático de dados digitais". **------- França, "Estratégia de Defesa e Segurança dos Sistemas de Informação", 2011**
"[…] o ambiente composto por elementos físicos e não-físicos, caracterizado pela utilização de computadores e outros dispositivos do espectro eletromagnético, para armazenar, modificar e trocar dados através de redes informáticas". **Manual de Tallinn sobre o Direito Internacional Aplicável à Guerra Cibernética da NATO, 2013**
"Ciberespaço: O ambiente global intangível onde ocorre a comunicação online entre pessoas, software e serviços através de redes informáticas e dispositivos tecnológicos". **Tribunal de Contas Europeu, "Desafios a uma política de Cibersegurança eficaz da UE", 2019**

Um contributo notável é o de Giles e Hagestad (2013), colocando a definição em perspetiva. Este estudo comparativo constata que o conceito de Ciberespaço difere ainda em termos semânticos, quando observada em idiomas como o chinês ou o russo. Contrariamente ao tratamento ocidental da palavra, que agrupa o Ciberespaço num domínio próprio, do russo киберпространство ou kiberprostranstvo e do chinês 網絡空間 ou Wǎngluò kōngjiān, a sua tradução apenas encontra proximidade à expressão *information space*, que em português se refere ao espaço de informação. Os autores acrescentam que "o termo em chinês com maior aproximação ao que se entende por "Ciberespaço" na língua inglesa é 虛擬主機, Xūnǐ zhǔjī, podendo ser traduzido, de forma simplista, para anfitrião virtual" (Giles & Hagestad, 2013, p.7). Esta questão revela que a própria interpretação e perceção do universo ciber é interdependente da cultura das coisas.

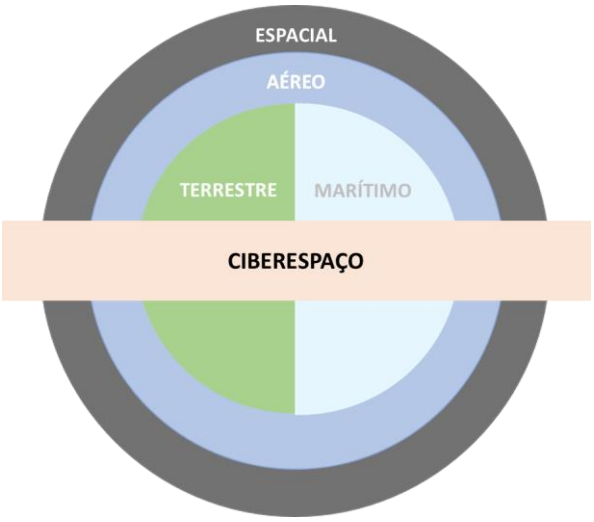
Estas são algumas formas de explicar o Ciberespaço tendo em conta a sua complexidade e ambiguidade. É de notar que existe uma grande multiplicidade de conceitos o que evidencia

substancialmente a transcendência deste universo que "possuindo características próprias (…) se distingue dos demais pela sua natureza imaterial, volátil, subjetiva e humana" (Honorato *et al.*, 2017, p. 10) e, mesmo entre especialistas, parece utópico um consenso relativo à sua abrangência.

Dito isto, e embora não seja reconhecida uma definição universal, podem ser identificadas ideias transversais à grande maioria das propostas oficiais apresentadas neste trabalho. Estão numeradas por ordem relevância, isto é, tendo em conta o número de vezes mencionadas:

1. Os dados e/ou o armazenamento, processamento, acesso, transmissão, troca e partilha de informação, valores e serviços; um espaço de comunicação;
2. A sua constituição interdependente e em rede, incondicionada por fronteiras físicas, associadas às TIC;
3. Espaço de Tecnologias de Informação;
4. Escala global que lhe confere uma enorme complexidade;
5. A conceção utópica de um universo intangível, paralelo ao mundo físico.

Figura 2. Representação alegórica do Ciberespaço



Fonte: Adaptado de (Honorato *et al*., 2017).

Assim, para efeitos da presente dissertação, tem-se como conceito operacional de Ciberespaço: o domínio de índole comum - transversal aos espaços tradicionais (Figura 2) mas também incorporado num universo transcendente -, composto por uma vasta rede interdependente de tecnologias de informação e comunicação à escala global, onde ocorre o

armazenamento, processamento, acesso, transmissão, partilha e intercâmbio de dados, serviços, valores e interações.

Conclui-se que o Ciberespaço, criado para integrar toda a nova atividade nascida a partir das últimas décadas do século XX, representa uma revolução em si, alterando continuamente o modo de viver, trabalhar, aprender e pensar, num outro espaço em que agora existimos, em certa medida, difícil de situar e delimitar. É retrato, portanto, de um conjunto de vivências num espaço associado às tecnologias e à computação, cuja diversidade de narrativas sugere que se trata de um conceito polissémico, melhor entendido como uma pluralidade ao invés de uma singularidade.

1.2.2 Geografia

As TIC assistiram a um avanço imenso, desde a sua criação aos tempos presentes, possibilitando um aumento expressivo das taxas de capacidade[5] e de transmissão da internet. Das componentes integrantes do Ciberespaço, a internet considera-se a sua principal rede de acesso (tendo em conta o crescimento exponencial do número de utilizadores à escala global nas últimas décadas), agora num espaço mais unificado que nunca.

Ora, a internet - da aglutinação dos termos *interconnected* e *networks* – pode definir-se como "[...] uma infraestrutura de redes de computadores que interliga, à escala global, um vasto e heterogéneo conjunto de equipamentos que assegura a comunicação em rede das aplicações aí instaladas e dos utilizadores que as utilizam" (Rodrigues, 2022, p. 6). Posto isto, atualmente é transmitida uma maior quantidade de informação, de acesso livre e descentralizado, a um ritmo progressivamente mais célere, sobretudo através da *World Wide Web* (www)[6] ou simplesmente *web*, o serviço da internet mais utilizado e o que mais tráfego gera. De facto, a utilização da internet assume um importante papel atuando como via de acesso a todo o tipo de informação, em tempo real, e "Sendo uma das principais forças motrizes da globalização e do progresso das comunicações, ela fornece meios inigualáveis de intercâmbio cultural, informativo e de ideias" (Fernandes, 2014, p. 11). Torna-se imperativo reconhecer que, na sociedade em rede "[...] o poder e a falta dele são avaliados em função do acesso a redes e do controlo dos seus fluxos a recursos, informacionais ou financeiros" (Elias, 2018, p. 301). Assim, para uma apresentação estruturada do tema, pensámos a questão da espacialidade como um ponto crucial a abordar e,

[5] Referente à capacidade produtiva, isto é, o número máximo de produtos ou serviços que se consegue produzir com os recursos disponíveis, num determinado período de tempo.

[6] Em português, Rede Mundial de Computadores, que consiste na "[...] possibilidade de aceder a conteúdos através de uma aplicação genérica específica, um *browser*" (Antunes & Rodrigues, 2022, p. 4)

como tal, usamos geografia do Ciberespaço para descrever a distribuição geográfica dos recursos digitais e das infraestruturas que compõem a internet tanto numa perspetiva europeia como mundial, representada nas Tabelas 2 e 3.

Tabela 2. População mundial e o uso de internet, por região mundial, em JAN de 2023

Regiões Mundiais	População (2023 Est.) (milhões)*	Utilizadores de internet (milhões)*	% de Penetração (% Pop.) *	Crescimento 2000 – 2023**
Ásia	4.442	2 766	62.4%	2.452%
África	1.443	596.1	41.4%	13.233%
Europa	744	673.3	90.5%	611%
América do Sul	438	353.2	80.7%	N/A
América do Norte	378	347.8	92%	222%
Médio Oriente	295	221.9	75.2%	6.194%
América Central/ Caraíbas	225	165.8	73.7%	2,858 %
Oceânia	45	35.7	79.3%	301%
Total:	8.01	5.16	64.5%	1.392

Fonte: Adaptado de *Digital 2023: Global Overview Report** e *Internet Usage Statistics***.[7]

A Tabela 2 fornece um conjunto de dados de janeiro de 2023 sobre os quais é possível argumentar, nomeadamente os utilizadores de internet distribuídos por regiões mundiais (África, América Central e Caraíbas, América do Norte, América do Sul, Ásia, Europa, Médio Oriente e Oceânia), a respetiva percentagem de penetração na população e o seu crescimento no período compreendido entre 2000 e 2023. Através da sua análise é possível constatar que os países asiáticos dominam o acesso à internet em número de utilizadores (2 766 dos 4 442 milhões cidadãos), porém, para uma avaliação rigorosa da distribuição dos seus utilizadores e a fim de traçar hipóteses válidas sobre o seu impacto nas sociedades, é crucial considerar a totalidade da população da região. Isto é, examinar o grau de penetração da internet nas

[7] Disponível em: Digital-2023-Global-Overview-Report.pdf e https://www.internetworldstats.com/stats.htm

respetivas regiões. Deste modo, a América do Norte é a região mundial com a maior taxa de acesso (347.8 milhões de utilizadores) representado cerca de 92% da sua população total, contrariamente à Ásia, cuja percentagem cai para os 62.3%.

Para além do mencionado, observa-se ainda que a taxa de crescimento de utilizadores de internet entre o período de 2000 a 2023 foi positiva em todas as regiões mundiais, em especial no continente africano. Com o maior crescimento percentual absoluto, África atingiu os 13,233%, precedida pelo Médio Oriente (6.194%) e a Ásia (2.452%).

Outrora, para além do contexto mundial, atendamos ao contexto europeu.

Tabela 3. Países europeus e o uso de internet, em JAN de 2023

Países Europeus	População (Est.) (milhões)	Utilizadores de internet (milhões)	% de penetração
Alemanha	83.31	77.53	93.1%
França	64.69	59.94	92.6 %
Itália	58.96	50.78	86.1 %
Espanha	47.54	45.12	94.9 %
Polónia	41.48	36.68	88.4%
Portugal	10.26	8.73	85.1%

Fonte: Adaptado de *Digital 2023: Local Country Headline Report*.[8]

Na tabela 3 estão representados 6 países europeus com algumas das maiores taxas de utilização de internet, em janeiro de 2023. Consta-se que todos eles (Alemanha, Espanha, França, Itália, Polónia e Portugal) possuem uma taxa parcialmente alta de utilização de internet em termos relativos, reflexo de um investimento tecnológico e uma adoção significativa da internet no quotidiano.

Estima-se que atualmente 5,16 mil milhões de pessoas acedem à internet em todo o mundo, correspondente a 64,5% da população total mundial. A análise dos dados apresentados nas tabelas sugere que o número de pessoas ligadas à internet tem vindo a aumentar a nível mundial, todavia, é de notar que o seu acesso representa uma variável constante, pelo que os valores apresentados carecem de uma interpretação ponderada.

[8] Disponível em: https://wearesocial.com/uk/blog/2023/01/digital-2023/

De acordo com o Relatório do *Digital 2023: Global Overview Report*, de 2023, apesar de a um ritmo consideravelmente mais lento do que o verificado durante a década de 2010, o total global de utilizadores aumentou 1,9% entre janeiro de 2022 e janeiro de 2023 . Aliás, para se considerar esta questão, é imprescindível mencionar a pandemia de COVID-19 como catalisador para a utilização do Ciberespaço (sobretudo entre os mais jovens) e, consequentemente, o seu desenvolvimento (Felgueiras *et al*., 2023). Neste sentido, pode afirmar-se ter sido um estimulante do processo de digitalização, e, de acordo com Oliveira (2020, p. 54), "[...] a pressão causada pela pandemia acelerou a revolução digital a que estávamos a assistir, fazendo com que acontecesse em poucas semanas uma transformação que, em condições normais, levaria provavelmente mais do que uma década".

Conclui-se que a utilização da internet, à escala universal, distribui-se de forma desigual (devido sobretudo às disparidades socio-económicas entre Estados e ao desenvolvimento das infraestruturas), numa geografia composta por redes e nódulos. Isto é, as novas tecnologias, transformadoras da relação com o espaço, permitiram a reconfiguração da geografia cunhada pela fronteira física e deram lugar à geografia em rede, que constitui uma das mais importantes noções do espaço hodierno. Por outras palavras, o Ciberespaço potencializou o surgimento de uma nova geografia, dinâmica, composta por nódulos de fluxos informacionais sendo sensato afirmar que geografia e tempo já não são fronteiras.

1.2.3 Ciberespaço e Segurança: a janela do crime

Se abrirmos uma janela, tanto entrará o bom como o mau.
[If you open the window, both fresh air and flies will be blown in.]

(Deng Xiaoping, em meados de 1980).

O advento da internet e a proliferação da tecnologia revelaram um carácter extremamente vantajoso em diversas matérias e o âmbito securitário não compõe uma exceção. Isto é, embora pesando de devida ponderação, pode afirmar-se que progressos tecnológicos refletem progressos na área da prevenção e investigação criminal (IC). Uma das vantagens facilmente identificáveis da utilização do Ciberespaço nesta matéria diz respeito à recolha de prova, facilitada face à possibilidade de rastreio de um conjunto de ações ocorrentes no ambiente ciber - como dados de dispositivos móveis, redes sociais, registos digitais - que poderão constituir um elemento-chave na condução de uma investigação.

O Ciberespaço oferece, ainda, novas ferramentas e métodos de recolha e análise de informações às autoridades (através, por exemplo, do processamento e análise de uma grande

quantidade de dados - *big data*[9]), possibilitando detetar padrões e tendências que possam indicar potenciais ameaças. Assim, com recurso às novas tecnologias de análise de dados é possível auxiliar operações de natureza preventiva, ou seja, monitorizar e identificar, em tempo real, atividades que denunciem uma ameaça securitária e, consequentemente, prevenir a ocorrência do crime. Tomam-se como exemplo intervenções no âmbito do tráfico de estupefacientes, seres humanos e armas, atividade terrorista e movimentos financeiros suspeitos.

Para além do referido, as tecnologias permitem o intercâmbio de informação sensível relevante entre indivíduos e organizações de modo quase imediato que, consequentemente, possibilita a cooperação internacional em matéria de segurança, enfrentando conjuntamente novos riscos e ameaças emergentes na nova arena internacional. Atualmente, muitas são as organizações de cibersegurança que instituem plataformas de partilha de informação para facilitar este processo cuja principal finalidade passa por detetar, prevenir, reprimir e investigar atividades ilícitas ou suspeitas.

Estes exemplos são apenas parte de um todo tendo em conta o vasto leque de oportunidades oferecidas pelo uso do Ciberespaço em matéria securitária. Reconhece-se a importância deste domínio para um aperfeiçoamento na eficácia e eficiência dos serviços e técnicas policiais no combate à criminalidade pelo garante de uma sociedade mais segura. Ainda assim, apesar de sinónimo de uma ferramenta vantajosa é facto que o seu carácter volátil, flexíloquo, de várias faces, se traduz também ele numa possível via para a prática de várias formas de crime num vasto universo de comportamentos desviantes.

Vejamos. Em 2011, o chamado "Silk Road" (em português, 'Rota da Seda') ficou conhecido como um dos primeiros mercados *online* na *dark web*, famoso pela venda de produtos ilícitos, nomeadamente drogas. Por sua vez, o dia 24 de novembro de 2014 marca a data em que a Sony Pictures, um gigante do setor do entretenimento, sofreu um ataque informático da autoria do grupo de *crackers*[10] *The guardians of Peace.* Dos cerca de 100 Terabytes de dados roubados, constavam informações pessoais dos funcionários, dados financeiros da empresa e informações sobre futuros lançamentos de produtos.

[9] De acordo com o Parlamento Europeu (2021)," Big Data" ou megadados refere-se à quantidade imensa de dados gerados através de pessoas ou máquinas, de forma instantânea, disponíveis para recolha e análise.

[10] De acordo com o dicionário enciclopédico online da Porto Editora, *cracker* designa uma "pessoa que quebra a segurança de sistemas informáticos e computadores alheios, geralmente com o objetivo de provocar danos, roubar dados"; pirata informático.

Também em maio de 2021, a *Colonial Pipeline*, uma das principais empresas de gasodutos norte-americana, sofreu um ataque de *ransomware*[11] - conduzido pelo grupo *Darkside* - que se traduziu na paralisação de um dos maiores oleodutos nos Estados Unidos e, consequentemente, na escassez de combustível em diversos pontos do país. Este caso ficou conhecido como um dos maiores incidentes do âmbito da Cibersegurança, no ano de 2021.

No caso português, toma-se como exemplo o ciberataque ocorrido a 27 de setembro de 2022, confirmado pelo Centro Nacional de Cibersegurança, envolvendo a rede do Ministério da Defesa Nacional (MDN) e do Estado-Maior-General das Forças Armadas (EMGFA) de onde terão sido extraditados centenas de documentos e relatórios da NATO - classificados como Secretos e Confidenciais - e, posteriormente, colocados à venda na *dark web*. São ainda do conhecimento público o caso de João, um aluno universitário de 18 anos que planeava um ataque à Faculdade de Ciências da Universidade de Lisboa a 11 de fevereiro de 2023, que utilizou a internet para obter armas e desenvolver um fascínio por assassinatos em massa e ainda a recente Operação "3P", uma operação de grande dimensão levada a cabo pela Polícia Judiciária (PJ) de combate à pornografia infantil na internet.

Os episódios acima retratados servem de ilustração para um problema de extrema gravidade que se desenvolveu face à popularização e sofisticação das TIC, que evidencia, de facto, a necessidade de tratamento do Ciberespaço enquanto matéria securitária. Isto é, sendo o Ciberespaço um elemento comum a uma panóplia de atividades humanas, faz-se acompanhar inevitavelmente do crime. Neste contexto internacional, não só se assiste à emergência de diferentes tipos de ameaças e crimes no novo[12] espaço (*Phishing*[13]*, malware*[14]*, blacklist*[15]*,* por exemplo), como se verifica uma tendência de migração de inúmeras ameaças da esfera tradicional para a rede cibernética "com novos métodos e ações ofensivas de grande

[11] Segundo o glossário online da ENISA (2024), "ransomware representa um tipo de malware (vírus, trojans, etc.) que infectam os sistemas informáticos dos utilizadores e manipulam o sistema de forma a que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados que estão armazenados. A vítima geralmente recebe um aviso de chantagem por pop-up, pressionando a vítima a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos".

[12] Apesar da sua origem datar os finais do século XX, o ciberespaço pode ser entendido como um "novo espaço" tendo em conta a sua magnitude e constante evolução. Há ainda um longo caminho a percorrer para o melhor entendimento sobre os benefícios e desafios a ele associados.

[13] "É o mecanismo de elaborar mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de emails ou mensagens de phishing para que estes abram anexos maliciosos, cliquem em URLs inseguros, revelem as suas credenciais através de páginas de phishing aparentemente legítimas, façam transferências de dinheiro, etc" (ENISA).

[14] "Programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima" (NIST, 2013, p. 118).

[15] "Uma lista de entidades discretas, tais como hosts ou aplicações, que foram previamente consideradas estarem associadas a atividade maliciosa" (NIST, 2013, p. 20).

envergadura lesivas do interesse nacional" (CNCS, 2019, p. 18), por exemplo, terrorismo, comércio ilegal, ofensa à integridade física, difamação, exploração sexual de menores, "provocando a deslocação do campo de batalha para o ciberespaço" (Martins, 2012, p. 32), contexto que tem justificado a securitização (do inglês *securitization*) do Ciberespaço, "com implicações legais, éticas e políticas" (Geraldes, 2019, p. 91).

A teoria de securitização, uma das principais contribuições da Escola de Copenhaga (1985), refere-se ao reconhecimento de uma matéria enquanto ameaça existencial e, consequentemente, assunto de segurança, numa determinada sociedade. Porém, importa referir que a ameaça é resultado de uma construção social que poderá, portanto, diferir consoante o ator que define (ou não) um assunto enquanto ameaça existencial (teoria construtivista). Quando esse assunto é considerado urgente e a ameaça legitimiza a violação de regras na realização de ações de emergência, dá-se a securitização (Buzan *et al*., 1998). Enquanto quebra das normas, pelo carácter de urgência que é atribuído a uma matéria, poderá ser vista como uma versão extrema de politização, considerada como uma falha da própria política.

A Cibersegurança resulta, deste modo, do cruzamento entre o Ciberespaço e a segurança e consta, atualmente, no topo das agendas políticas estatais e das organizações internacionais em matéria de segurança e defesa, atendendo ao seu grau de urgência e notoriedade. E apesar carecer de uma definição universalmente aceite, para efeitos da presente dissertação tem-se como Cibersegurança:

> Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem (CNCS, 2019, p. 7)[16].

À sociedade do risco[17] acresce-se a apreensão com o Ciberespaço, tendo em conta os riscos e obstáculos a ele associados. Assim, o objetivo deste capítulo passa por reconhecer que ao Ciberespaço se soma uma necessidade securitária, sinónimo não só de oportunidades como

[16] Disponível em: https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

[17] O risco é inerente a qualquer atividade humana, em muito exacerbado face à cultura do medo e insegurança (Beck, 1992) que se faz impor na contemporaneidade. "Sociedade do risco", é por isso, uma das designações que melhor descreve a sociedade atual quando avaliado o panorama geral em matéria de segurança.

de um conjunto de desafios. Um deles diz respeito à exploração sexual de menores, tema devidamente aprofundado no capítulo que se segue.

Capítulo 2 - Exploração sexual de menores no Ciberespaço

2.1. As e-ameaças: o caso da exploração sexual de menores

Num mundo que teima em não parar de mudar (Guedes, 2006) confrontamo-nos com ameaças profundamente atípicas, agora mais complexas do que nunca. As ameaças ditas tradicionais conheciam um espaço geográfico devidamente localizado e "eram originadas por adversários politicamente identificados" (Elias, 2011, p. 118). No entanto, fruto do impulso da globalização e das mudanças no contexto internacional, as *novas* ameaças ganham espaço e a delinquência moderniza-se. Assim, compreende-se a utilização da expressão "novas ameaças" para designar aquelas que são alvo, atualmente, de uma maior preocupação por parte dos cidadãos, Estados e comunidade internacional opondo a expressão "velhas ameaças" referentes àquelas prioritárias há cerca de uma ou mais décadas (Borges, 2009). Porém, a discussão sobre a aparente antítese entre as "novas" *e as* "velhas" é fundamental para se compreender o seu espectro, isto é, podemos reconhecer que parte destas novas ameaças são melhor entendidas como velhas ameaças que surgem com nova roupagem.

Uma das várias ameaças que tem atraído progressivamente a atenção global, que se acentua face à constante globalização das TIC, são, sem dúvida, as e-ameaças. Contudo, seria prematuro explorar o tema sem primeiramente dar uma breve noção de "ameaça", para sua melhor compreensão.

De acordo com o proposto por um relatório[18] das Nações Unidas (2004, p. 25) em matéria de segurança, uma ameaça – no âmbito das relações internacionais – pode ser hoje entendida como "Qualquer acontecimento ou processo que conduza à morte em larga escala ou à diminuição da probabilidade de vida que comprometa os Estados enquanto unidade basilar do sistema internacional [...]". Na ISO/IEC 27032 de 15 de julho (2012, p. 7) entende-se por ameaça uma "potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização".

Um conjunto de outros aspetos deverão ser tidos em consideração para um melhor entendimento do seu significado. A primeira é que uma ameaça assenta numa hipótese meramente probabilística tendo em conta que a sua ocorrência não é uma certeza, apenas indica que existe um perigo iminente com consequências adversas prováveis de ocorrer. Outro

[18] *A more secure world: Our shared responsibility.* Report of the High-level Panel on Threats, Challenges and Change (2004). http://providus.lv/article_files/931/original/HLP_report_en.pdf?1326375616

ponto a destacar é a diferenciação entre ameaça e risco, porque apesar de próximos e, por vezes, incorretamente confundidos, os conceitos distinguem-se. Segundo a ONU, no "Manual de Política de Segurança" (2017, p. 67) risco pode definir-se como a "probabilidade de ocorrência de um acontecimento prejudicial e as suas respetivas consequências, caso aconteçam". Por outras palavras, o risco pode entender-se como a estimativa de concretização de uma determinada ameaça, face às vulnerabilidades dos ativos em causa e do sistema de segurança por ela exploradas, tendo em conta as consequências adversas que daí poderão resultar. Isto é, a ameaça constitui um dos 4 fatores estruturantes do risco – é, portanto, dele indissociável – porém, difere-se de um sinónimo.

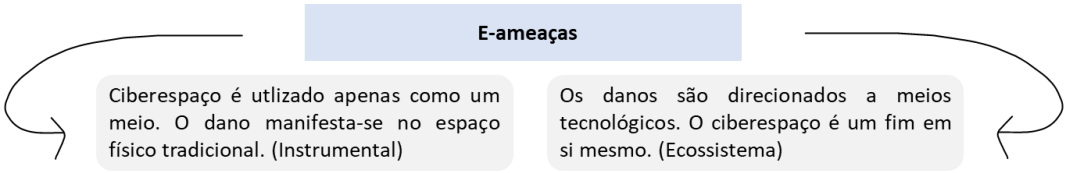
É ainda imprescindível considerar os contextos sociais nos quais as ameaças ocorrem uma vez que nem todas as sociedades partilham necessariamente as mesmas perceções sobre a segurança e as suas causas subjacentes (como exposto no subcapítulo 1.2.3 referente à teoria da securitização). A consideração de uma matéria enquanto ameaça existencial e o risco subjacente à sua ocorrência variam, desde logo, de acordo com uma série de fatores desde a posição geográfica, condição política e estratégica como as próprias normas e valores culturais de um Estado-Nação.

Nas palavras de Creppel (2011, p. 451) "Uma ameaça é comparada a uma casa em chamas, onde a urgência do perigo é palpável", dividida em três *entities* "ameaças físicas, ameaças económicas e ameaças cibernéticas" (Urinov, 2020, p. 156). Tal significa que o surgimento do Ciberespaço adapta o conceito de ameaça à sua dimensão, designada por ciberameaça ou e-ameaça (do inglês *e-threat*). A designação "e-ameaça" deriva da conjugação da palavra "ameaça" com o prefixo "e" que, como explorado no subcapítulo 1.2.1, cunha a palavra, assim como muitas outras (*e-commerce, e-learning, e-mail*) ao universo transcendente, para se referir à atividade ocorrente no Ciberespaço; à ameaça que navega pela internet. E embora a sua definição varie, no contexto do presente trabalho de investigação, utilizamos e-ameaça para nos referirmos a qualquer fator, acontecimento ou ação (em curso ou previsível), que ocorre no Ciberespaço, com o potencial de "causar dano à integridade das pessoas, seres ou coisas" (Granjo, 2006, p. 1168) seja ele um dano material ou moral, de natureza variada (social, económica, política). O conceito pode ainda ser percecionado em função da intenção de provocar um resultado e a capacidade de o executar.

As e-ameaças caracterizam-se, essencialmente, "pela sua transversalidade, rápida propagação em rede, anonimização e persistência" (CNCS, 2019, p. 18). Porém, importa sublinhar que as e-ameaças comportam em si duas realidades. Isto é, como observável na Figura

3, a utilização do Ciberespaço para a prática de crime poderá representar tanto um fim em si mesmo na medida em que é nele praticado o delito e as consequências derivadas são também elas balizadas ao Ciberespaço (direcionadas aos meios tecnológicos) como um meio cujo objetivo será provocar dano ou uma consequência adversa contra bens jurídicos não digitais (pessoas, seres ou coisas) no espaço tradicional físico – Ciberespaço enquanto um recurso meramente instrumental; que "[...] se traduz em crimes de índole comum" (Rodrigues, 2022, p. 77), como é o caso da exploração sexual de menores online. Esta forma de crime enquadra-se no perfil de e-ameaça, encontrando-se qualquer abusador à distância de um clique na procura por informações e dados sobre o perfil de uma potencial vítima e da ocasião em que se fará o contacto. O Ciberespaço é aqui utilizado como meio de aproximação entre estes dois atores em cena (abusador e vítima), bem como facilita o acesso e difusão de conteúdo pornográfico infantil e que, assim, se perpetue este tipo de crime.

Figura 3. Representação dos tipos e-ameaças



A exploração sexual de menores *online* consta, atualmente, como uma prioridade para a ONU - referida na Convenção sobre os Direitos das Crianças (1989) - para a UE - presente na Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas (EMPACT), onde constam as principais prioridades na luta contra a criminalidade para o período de 2022-2025, em relatórios da Europol (*Internet Organised Crime Assessment* (2023), *Spotlight Report on Child Sexual Exploitation* (2023)), em Diretivas (Diretiva n.º 2011/92/UE do Parlamento Europeu e do Conselho de 13 de Dezembro de 2011, revisto em 2022), em Estratégias (Estratégia europeia para uma Internet melhor para as crianças (2012), Estratégia da UE para uma luta mais eficaz contra o abuso sexual das crianças (2020)) - e para Portugal, (este último presente no Relatório Anual de Segurança Interna (2022) para o período de 2022 a 2025), ganhando crescentemente palco no cenário de segurança internacional face ao acentuado aumento que tem verificado ao longo dos anos.

Por conseguinte, é uma e-ameaça a combater que merece a devida atenção.

2.2. Problematização

Dadas as oportunidades oferecidas pelos avanços na tecnologia e internet, umas diversidades de crimes tornam-se, hoje, muito mais facilmente praticáveis e extensíveis a qualquer indivíduo independentemente da sua condição, onde é enquadrável a exploração sexual de menores no Ciberespaço. Após uma extensa análise documental, que passou pela leitura das principais diretivas, recomendações, decisões e outros atos legislativos, bem como os principais relatórios (nacionais e internacionais) que mencionam este tema como uma ameaça a combater, conclui-se que para "exploração sexual de menores online" não existe nenhuma definição internacionalmente acordada atendendo a variantes como a idade do menor, tipo de práticas que são consideradas abuso sexual, entre outras (Magalhães, 2016). Como tal, apresentam-se propostas de organizações e autores que exploraram esta temática.

De acordo com o Modelo de Legislação contra o Tráfico de Pessoas da *United Nations Office on Drugs and Crime* (UNODC, 2009, p. 20), a exploração sexual tem-se como "a obtenção de benefícios financeiros ou outros, através do envolvimento de outra pessoa na prostituição, escravatura sexual ou outros tipos de serviços sexuais, incluindo atos pornográficos ou a produção de materiais pornográficos". Albuquerque (2010) diz-nos ainda que a exploração sexual consiste na instrumentalização do corpo da vítima como objeto de prazer sexual, "podendo aí integrar-se qualquer outro tipo sexual de crime" (Ribeiro, 2022).

À exploração sexual de menores soma-se a particularidade de ser cometido contra um menor, na qual a *National Society for the Prevention of Cruelty to Children* (NSPCC) enquadra o abuso sexual. Nesta forma de abuso, a criança[19] ou adolescente é coagida, manipulada ou forçada à prática de atividades sexuais por um indivíduo ou grupo, em troca de presentes, drogas, dinheiro ou afeto. A Diretiva n.º 2011/92/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, define no art. 4º algumas infrações relativas à exploração sexual de crianças, permitindo adotar uma visão mais clarificada sobre aquilo que poderá integrar, do ponto de vista legal, comportamentos que identifiquem esta forma de crime:

> "2. Induzir ou recrutar uma criança para participar em espectáculos pornográficos, ou explorar uma criança para tais fins, como fonte de rendimento ou de qualquer outra forma[...];
>
> 3. Coagir ou forçar uma criança a participar em espectáculos pornográficos, ou ameaçar uma criança para tais fins[...];

[19] Como criança, segundo o CP, tem-se qualquer menor com idade inferior a 14 anos.

> 4. Assistir com conhecimento de causa a espectáculos pornográficos em que participem crianças [...];
>
> 5. Induzir ou recrutar uma criança para participar em prostituição infantil, ou explorar uma criança para tais fins, como fonte de rendimento ou de qualquer outra forma [...];
>
> 6. Coagir ou forçar uma criança a participar em prostituição infantil, ou ameaçar uma criança para tais fins [...]
>
> 7. Praticar actos sexuais com uma criança com recurso à prostituição infantil [...].”

Este crime não é recente, enquadrando-se na tipificação de ameaça tradicional, alvo de preocupação anterior a 2000, na comunidade internacional. Toma-se como exemplo a Convenção sobre os Direitos das Crianças datada em 1989, cuja principal finalidade seria estabelecer os direitos fundamentais de crianças e jovens de idade inferior a 18 anos, no direito internacional. Outrora, as mais recentes análises do fenómeno por parte de organizações que se dedicam a esta temática demonstram uma tendência de crescimento acentuado da ESM – em termos quantitativos e em grau de gravidade (Europol, 2023) - que, atualmente, assume uma nova personalidade: a vertente *online*, alvo de estudo na presente dissertação. Recuando a 2012, os dados da *Internet Watch Foundation* (IWF) revelam que nesse ano foram confirmadas 9 550 páginas *web* integrando conteúdo de ESM em todo o mundo, um contraste colossal com o ano de 2022: dez anos passados e os números disparam abruptamente para os 255 571. E como justificamos estes valores?

Ora, de acordo com o que nos é apresentado por Ferraro *et al.* (2005), no período anterior à internet, um adulto que tencionasse levar a cabo este tipo de crime rapidamente procuraria enquadrar-se num ambiente de exposição direta a menores, como é caso dos programas de voluntariado que trabalham com crianças, a habitação em bairros familiares (através do desenvolvimento de relações de amizade com crianças da vizinhança) ou até desempenhar atividades profissionais que exigem um contacto diário e próximo das mesmas.

Porém, o advento das TIC, nomeadamente a internet, proporcionou a formação de uma rede mundial de comunicações ilimitadas, sem fronteiras ou restrições horárias que, muito embora não fosse concebida para perpetrar atividades criminosas, é inevitavelmente utilizada para criar e disseminar conteúdos abusivos (APAV, 2021). Este facto possibilitou uma variedade de *modus operandi*[20], não sendo mandatória, nos dias correntes, a presença física do abusador no meio da criança - com recurso (ou não) ao contacto físico - (abuso sexual offline), como já

[20] Do latim, “modo de atuação”.

"[…] pode configurar a persuasão ou coação da criança para enviar ou publicar imagens sexualmente explícitas de si mesma, participar em atividades sexuais através de câmaras *web* ou smartphones ou manter conversas de teor sexual" (Fernandes, 2018, p. 82) (abuso sexual *online*). Uma vez na Internet, estes conteúdos podem, com inúmera facilidade, ser difundidos para outros destinatários via-email ou com recurso às redes sociais, partilhados em websites, vendidos e comprados *online* sem o conhecimento ou consentimento da(s) vítima(s), semelhante à propagação de um vírus informático.

Cooper (2009, p. 106) enuncia cinco tipos de exploração sexual de crianças: prostituição intrafamiliar, pornografia de menores, aliciamento *online* para encontros sexuais, turismo sexual infantil e tráfico de crianças para escravatura, trabalho, prostituição ou outras violações dos direitos civis. De acordo com o regime normativo europeu, inclui-se ainda a posse ou intenção de adquirir conteúdo digital referente à ESM, a sua oferta e distribuição ou qualquer outro método que a torne possível, nomeadamente a sua produção ou a colaboração.

Toda esta conjuntura decorre de um fator: as oportunidades oferecidas ao crime pelo Ciberespaço. Como tal, o próximo capítulo pretende entrar em maior detalhe sobre o que justificará, na sua grande maioria, o problema global do ESM *online*.

2.3. Desafios e características

Para um melhor enquadramento da ESM *online* é imperativa a consciencialização sobre o que enfrentamos, isto é, sobre as particularidades do Ciberespaço não só alusivos à exploração sexual de menores *online* mas também comuns a outros crimes nele ocorrentes. Para tal, serão sumariamente explorados alguns dos obstáculos à investigação criminal apontados como mais desafiantes. Primeiramente abordamos a questão da espacialidade e tempo, ou seja, a sua geografia de redes e nódulos. Posteriormente, a internet como um instrumento de encobrimento de atividade ilícita, onde será abordado o tema da *dark web* em articulação com o anonimato. Por fim, será explorada a problemática da governação do Ciberespaço.

2.3.1 Ciberespacialidade e cibertempo

Como suprarreferido, o espaço ciber considera-se a passagem da condição offline para *online*, não sendo a presença física um imperativo para a construção de relações sociais (por *e.g.*), ou, neste caso, levar a cabo uma ação criminosa contra menores. Isto é, "nas comunidades

virtuais, as pessoas fazem praticamente tudo o que se fazem na vida real, apenas deixamos os nossos corpos para trás" (Rheingold, 1993, p. 3).

O seu espírito aberto e descentralizado, despido de barreiras espaciais ou temporais, confere-lhe uma personalidade complexa, quando transportada ao domínio da (in)segurança, desafiando a *law enforcement* na deteção desta ameaça e sua prevenção. Este crime que emerge na rede ramifica-se e assume, na contemporaneidade, um teor transnacional, detendo capacidade de alcançar uma geografia extensível a todos os cantos do mundo. Neste universo, "[...] os agentes criminosos têm oportunidade de aceder a um grande número de potenciais vítimas, esconder a sua identidade, atividades ilícitas e desenvolver a criminalidade a uma escala maior que nunca" (Felgueiras *et al.*, 2023, p. 1) ultrapassando as fronteiras fisicamente impostas pelos Estados (desprovidos, maioritariamente, de pensamento geográfico).

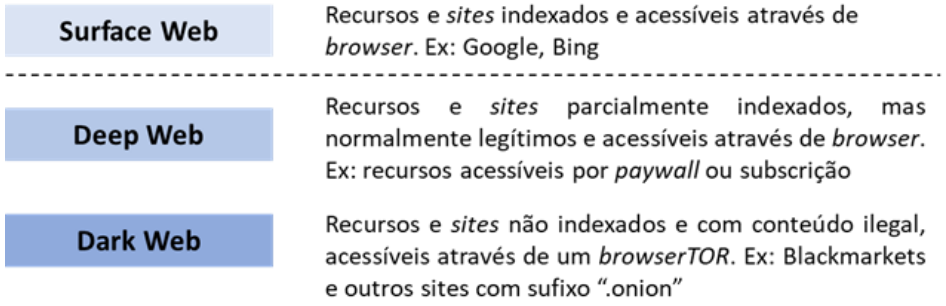
Enfrentamos uma presença assimétrica, imediata, em todo o lado, agora e para sempre. Isto é, a própria dimensão temporal adapta-se a uma nova condição: a do "agora" ser também ele permanente. Apesar de atualmente existirem mecanismos que impeçam a propagação de conteúdos de teor sexual não consentido, poderá afirmar-se que qualquer vídeo ou fotografia permanecerá infindavelmente neste espaço, já o enunciava a célebre frase: "Uma vez na internet, para sempre na internet". Prova vívida desse facto são as muitas das imagens atualmente em circulação na internet, produzidas há mais de 10 anos.

Acrescenta-se ainda a problemática da imprevisibilidade quanto à sua forma, tempo e local de ocorrência. De acordo com Elias (2011, p. 29), esta matéria pode ser associada ao princípio da incerteza das ciências matemáticas de Heisenberg "transportada igualmente para questões de segurança, para ameaças e riscos que afetam o mundo moderno", criando-se uma dúvida permanente sobre o modo e local onde podem ocorrer crimes graves e violentos, como é exemplo a exploração sexual de menores no Ciberespaço.

2.3.2 Anonimato

Como anteriormente percecionado, a internet considera-se a principal rede de acesso ao Ciberespaço, sobretudo através da *World Wide Web* (www) ou simplesmente *web*, o serviço da internet mais utilizado e o que mais tráfego gera. O serviço *web* é frequentemente dividido em 3 categorias, ordenadas pelo seu grau de permeabilidade e acesso: *surface web*, *deep web* e *dark web*, representado na Figura 4.

Figura 4. As camadas do serviço web



Fonte: Adaptado de Rodrigues (2022, p. 233).

A explicação mais comum compara as camadas da *web* a um iceberg. No topo a camada mais superficial e visível, de acesso direto pelos seus utilizadores através de *browsers* como a Google, Bing e Yahoo. É composta por páginas que incluem *sites* de notícias, redes sociais, *blogs*, lojas virtuais e outros tipos de conteúdo público e acessível a qualquer um que faça uso da internet. Porém, esta camada representa apenas uma pequena fração da internet total, na sua maioria composta por conteúdo não indexado e não acessível por meio de motores de pesquisa comuns, que compõem a chamada *deep web* - não visível, de maior dificuldade de acesso. Estima-se que representa mais de 90% de toda a *web* (Basheer & Alkhatib, 2021) utilizada muitas vezes para fins legítimos, caso dos bancos, jornalistas, ativistas políticos, agências de *law enforcement* e fins académicos e é igualmente denominada por *invisible web* que, na tradução para o português, significa um espaço invisível. Por fim, a última camada - *dark web* – abrangida pela anterior, e caracterizada pelo uso de software de criptografia especial para ocultar identidades e endereços IP dos utilizadores.

Outrora, "o enorme passo que a internet proporcionou na partilha de informação à escala global esconde um vasto leque de ameaças à segurança e à integridade dos dados que aí são processados" (Rodrigues, 2022, p. 43). A começar com a quase inexistente preocupação com a segurança no desenho da internet juntamente com o exponencial número de utilizadores que a acedem e que fazem dela um meio complexo, alvo de redes criminosas que encontram na sua estrutura uma possibilidade de explorar vulnerabilidades e com isso desenvolver a sua atividade. A *dark web* é, na sua esmagadora maioria, um meio para o desenvolvimento de atividades ilícitas, funcionando como um espaço comercial (composto por compradores e vendedores) e uma plataforma de disseminação de informação e comunicação entre criminosos que cooperam entre si - "Na darknet, os hackers compartilham informação entre si constantemente e aprendem uns com os outros" (Zenebe *et al*., 2019, p. 174) - facto que comporta uma maior

impermeabilidade às forças de autoridade. Nela se integram um conjunto de utilizadores com diferentes níveis de experiência técnica de computação e diferentes propósitos, onde se enquadra a prática de um vasto número de crimes como a exploração sexual de menores e muitos outros[21].

O que justifica a tamanha atratividade do crime pela *dark web*? Uma das grandes vantagens facilmente identificadas é a anonimização, "uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa" (Google, 2023), que consiste em "'esconder' o endereço IP origem de ligação (o nosso computador) ao longo do caminho até ao servidor em causa" (Rodrigues, 2022, p. 235). Distinguem-se, para o efeito, dois tipos de anonimato: pseudo anonimato e verdadeiro anonimato (du Pont, 2001). A comunicação pseudo-anónima é inerentemente rastreável (Rigby, 1995), isto é, embora a identidade do remetente da mensagem não seja facilmente localizável e disponibilizada por definição, é possível identificá-la. Contrariamente, uma comunicação verdadeiramente anónima é indetectável, o que levanta numerosas problemáticas. Embora o anonimato se revele de extrema importância na protecção do direito à privacidade, é também ele um desafio em si, permitindo no segundo caso, a prática do crime sem possibilidade de deteção (Akdeniz, 2002) o que resulta numa desresponsabilização por ações individuais.

Esta condição é passível de revelar mais facilmente os impulsos maliciosos de um indivíduo, premissa sustentada por Suler *et al*. (1998, p. 277) "será que um maior anonimato resulta num maior desvio? Porque um maior anonimato está normalmente associado a uma menor responsabilização pelas próprias acções, a resposta parece ser sim". Assim, o ambiente *online*, mais precisamente a *dark web*, abre portas ao indivíduo sem rosto, camuflado, que se traduz numa das maiores dificuldades no âmbito investigação de exploração sexual de menores e "é com sentido de compromisso que se deve olhar para a internet, na medida em que os largos benefícios que nos traz terão de ser continuamente avaliados em função dos riscos associados" (Rodrigues, 2022, p. 43).

2.3.3 A "terra de ninguém"

Na contemporaneidade, quem detém poder sobre a Segurança? Na nova ordem internacional moderna e atual, a autoridade estatal é contestada por um conjunto de atores

[21] Extorsão; sabotagem; roubo de dados; tráfico de estupefacientes e de armas; tráfico de seres humanos; recrutamento, radicalização e planeamento de ações terroristas; assassínio por encomenda; tráfico de meios digitais pirateados; falsificação de documentos; fraude (Basheer & Alkhatib, 2021).

face à sua incapacidade de monopolizar o conceito e práticas securitárias o que, por conseguinte, lhes tem retirado exclusividade na produção e manutenção da segurança. Assim, conta na atualidade com a participação de um conjunto de novos atores: para além das instituições públicas, as instituições privadas, a própria sociedade civil e organizações internacionais (quer de natureza intergovernamental quer supranacional). Esta questão poderá ser transportada para o domínio do Ciberespaço que, por si, passa a ser entendido como uma arena onde "desfilam e atuam vários atores com capacidades e interesses diferenciados" (Vales, 2020, p. 34).

Ora, quando abordado o tema da soberania sobre o Ciberespaço é imprescindível ter em conta dois aspetos distintos. Como anteriormente aprofundando, o Ciberespaço é melhor entendido como uma pluralidade ao invés de uma singularidade, tendo em conta a sua natureza *ubīquu*[22] - tanto integra uma componente física, transversal a outros espaços tradicionais, como se manifesta no virtual. E se o exercício do Direito é determinado pelas fronteiras físicas de um Estado e todo o espaço onde é exercida soberania estatal, por conseguinte, a resolução das questões inerentes à infraestrutura física do Ciberespaço parece ser facilitada: o exercício de poder é atribuído consoante a localização geográfica destas estruturas. Por outro lado, o seu cariz virtual suscita desafios mais complexos. Tal como referiu Gouveia (2023) no "II Congresso Luso-Brasileiro de Direito Internacional Público", para se verificar a presença de crime, neste caso a ESM *online*, é necessária a aplicação de direito penal ("qual?"). E com ela se arrastam muitas outras questões: "quem é o agente do crime?"; "onde está?"; "onde cometeu o crime?", "onde deverá ser julgado?". Isto é, em razão da sua arquitetura, faz-se emergir o dilema relativo à regulação do Ciberespaço e governança da internet, visto que (Lessig, 1999):

> [...] aqueles cujo comportamento está a tentar controlar [o Estado] podem estar localizados em qualquer lugar (ou seja, fora do seu lugar) na Rede. Quem é alguém, onde está, e se a lei pode sobre ele ser exercida - todas estas são questões a que o governo deve responder se quiser impor a sua vontade. Mas estas questões são em muito dificultadas pela arquitectura do espaço (p. 19).

Pela senda de Mueller *et al*. (2004, p. 4) "governança da internet" pode definir-se como uma "Ação colectiva, pelos governos e/ou operadores do sector privado de redes TCP/IP, afim de estabelecer regras e procedimentos para se fazer cumprir as políticas públicas e resolver disputas que envolvam múltiplas jurisdições". Por sua vez, um dos principais fóruns internacionais dedicado ao tema, o *World Summit on Information Society (2003)* descreve-o:

[22] Do latim, "que está em toda a parte".

> Os governos, bem como o setor privado, a sociedade civil e as Nações Unidas e outras organizações internacionais têm um importante papel e responsabilidade no desenvolvimento da Sociedade da Informação e, consoante o caso, nos processos de tomada de decisão. Construir uma Sociedade da Informação centrada nas pessoas representa um esforço coletivo que requer cooperação e parceria entre todas as partes interessadas.

Questiona-se, para o efeito: quem regula o Ciberespaço? Das demais tentativas de dar resposta a esta questão, "A Declaração de Independência do Ciberespaço" de Barlow (1996) ganhou reconhecimento. O Ciberespaço é nela descrito como "a nova casa do pensamento" e a internet como transcendente dos limites estatais e, portanto, naturalmente independente da sua regulamentação. É antes uma iniciativa e compromisso da sociedade civil que se organiza em comités, organizações, comunidades, que utilizam o diálogo para discutir um conjunto de normas à qual esta deve estar vinculada (Moreira, 2023).

Trachtman (1998) sustenta a ideia de neutralidade, que pode ser entendida como a atribuição, ao Ciberespaço, de um rótulo de "zona cinzenta" para efeitos de delegação de competências. Isto é, uma soberania partilhada pela comunidade internacional, não limitada pela esfera pública ou privada, civil ou militar, interna ou externa. Este argumento conduz à ideia de um espaço a que a todos pertence e se traduz, na prática, na "terra de ninguém". A condição de anomia, é este o grande desafio.

2.4. Enquadramento Jurídico

Ao nível internacional, importa reconhecer a Convenção das Nações Unidas sobre os Direitos da Criança (CDC) (1989) como o principal instrumento existente no domínio da proteção dos direitos das crianças onde se insere o combate a todas as formas de exploração e violência sexual (*e.g*. rapto, venda e tráfico de menores).

O tema da exploração sexual das crianças é igualmente abordado no Protocolo Facultativo à Convenção sobre os Direitos da Criança Relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil (2000), prevendo a criminalização de factos relativos à venda, prostituição e pornografia de menores - incluindo a tentativa - assim como incentiva a cooperação e assistência internacional neste âmbito.

A Convenção sobre Cibercrime do Conselho da Europa (2001), também intitulada de "Convenção de Budapeste", criminaliza no art. 9º a pornografia infantil quando, para o efeito,

se faça uso de um sistema informático, abrangendo tanto a produção, oferta, obtenção como posse deste tipo de conteúdo. Acresce a Convenção do Conselho da Europa Relativa à Luta contra o Tráfico de Seres Humanos (2005) que vê contemplada uma definição de tráfico de seres humanos, com especial enfoque nas vítimas de idade inferior a 18 anos no seu art. 4º, constituindo esta uma forma de exploração sexual nos casos de tráfico para esse fim.

Mais tarde, em 2007, foi ainda criada a Convenção de Lanzarote e em 2011 a Diretiva da União Europeia sobre Combate ao Abuso Sexual e Exploração Sexual de Crianças e Pornografia Infantil (Diretiva n.º 2011/92/UE) com o objetivo de reforçar a proteção de crianças e jovens, vítimas de exploração sexual, fomentando a cooperação nacional e internacional contra a esta forma de criminalidade que recorre às TIC.

Já em legislação nacional, a CRP é imprescindível de mencionar visto que nela são assegurados os direitos, liberdades e garantias fundamentais do cidadão, inteiramente violados pela prática de atos sexuais com crianças como explanado, por exemplo, nos art.º 25 e 26. O primeiro sob epígrafe "Direito à integridade pessoal", visando no nº 1 que "A integridade moral e física das pessoas é inviolável" e "Ninguém pode ser submetido a tortura, nem a tratos ou penas cruéis, degradantes ou desumanos" (nº 2). O art. 26º "Outros direitos pessoais", por sua vez, refere no nº 1 que "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação".

Por outro lado, o Código Penal estabelece na Secção II, Cap. V "Dos crimes contra a liberdade e autodeterminação sexual", Título I "Dos crimes contra pessoas", as disposições sobre crimes contra a autodeterminação sexual de menores (art. 171º a 179º). Ressalva-se que os atos sexuais praticados com ou em menor de 14 anos, perante a lei portuguesa, tipificam um crime suscetível de prejudicar o livre desenvolvimento da personalidade da criança na esfera sexual e psicológica e, por essa razão, são punidos mais gravemente. O legislador pretende, assim, assegurar a liberdade à autodeterminação da criança e os perigos inerentes ao envolvimento prematuro em atividades sexuais visto que, ainda que com consentimento, não lhe é reconhecida capacidade ou maturidade para a considerar uma decisão livre. Por outras palavras, protege-se o direito de ser criança.

Capítulo 3 - Aquisição e valoração da prova digital no Ciberespaço

3.1. Da prova digital

3.1.1 Conceitos

Como discutido nos capítulos anteriores, os avanços das tecnologias de informação germinaram uma nova criminalidade, globalizada e despersonalizada, cuja proliferação se faz notar ostensivamente. De facto, a ascensão da tecnologia introduziu mudanças no plano jurídico-legal, adaptando o âmbito da prova ao digital, numa tentativa de responder às necessidades da sociedade atual no combate às novas formas de crime que requerem "[...] uma nova tipificação no que diz respeito ao seu meio probatório" (Almeida, 2014, p. 9). Para bem nos inserirmos no cerne do objeto de estudo do trabalho, interessa determinar o que se entende por prova digital, e como tal, foi realizada uma pesquisa neste sentido.

Ora, tratando-se de um passado um tanto recente, identificámos que o conceito é ainda pouco explorado ao nível nacional e o leque de contributos nesta matéria é, contrariamente ao expectável, reduzido em virtude da sua dimensão, carecendo de aprofundamento tanto na comunidade académica como por parte do Estado face à ausência de uma definição legal de prova digital. Outrora, foram identificados, para o efeito, alguns contributos tanto ao nível nacional como internacional.

Rodrigues (2009, p. 39) define prova eletrónico-digital como "[...] qualquer tipo de informação, com valor probatório, armazenada [em qualquer dispositivo de armazenamento digital] ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital".

Ramos (2014, p. 86), por sua vez, define-a como "[...] informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. [...] [a] prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta". De modo mais conciso, Fidalgo (2020), descreve-a "no essencial, a prova digital é composta por uma sequência de *bits* e existe independentemente do suporte material no qual se encontre incorporada".

Também nas palavras de Mesquita (2010, p. 84-85), "[a] temática da prova electrónica (…) compreende a prova que se apresenta na forma digital, e não em suporte papel ou outro meio tangível, (e) compreende uma constelação de problemas que exige uma reconstrução

concetual complexa, com um enquadramento teórico que se adapte à rotura epistemológica introduzida pelas novas tecnologias no processamento, captação e memória das comunicações".

No plano internacional, o Regulamento (UE) n.º 910/2014 define documento eletrónico como "[...] qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual". Efetivamente, a prova digital considera-se um tipo de documento (um documento eletrónico) "[...] que deve ser entendido como todo o suporte digital que registe informação" (Lambelho, 2022, p. 24). O documento eletrónico assume um novo formato de documento que embora não conste no CPP, para efeitos probatórios e de acordo com Martins (2019), pode ser equiparado ao escrito. Sendo este último um meio de prova (constante no Cap. VII, Título II sob epígrafe "Dos meios de prova", Livro II "Da prova" do CPP), também a prova digital deverá permitir demonstrar um facto ou a existência de um ato jurídico, que se distingue dos demais pela característica do formato digital.

Recuando ao ano de 1999, também o *Scientific Working Group on Digital Evidence* (SWGDE), órgão do FBI, oferecia a definição de "Informação de valor probatório armazenado ou transmitido em formato digital".

De facto, este novo formato de prova assume extrema importância no cenário criminal nacional e internacional, revestida da capacidade de abraçar um número incalculável de conteúdos extremamente úteis na resposta a certo tipo de crimes. Para o efeito, podem ser identificados alguns tipos de prova digital: dados informáticos[23] (por *e.g.*, mensagens de SMS e de correio eletrónico; histórico de pesquisa; imagens de videovigilância), dados de tráfego[24] (endereço de IP), escutas telefónicas[25] e a localização celular[26]. Salvo quando a lei não o permite, qualquer vídeo ou áudio e todos os dados de rede podem ser utilizados como prova, permitindo, assim, a celeridade da descoberta da verdade material. É, indiscutivelmente, uma "[...] ferramenta insubstituível para a resolução de casos que, de outra maneira, não se solucionariam" (Costa, 2017, p. 69).

[23] Dispostos no art. 2.º, alínea b) da LC como "qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função".

[24] Dispostos no art. 2.º, alínea c) da LC como "os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente".

[25] Constante no Cap IV, Título III, Livro III do CPP.

[26] Constante no art. 252.º-A do CPP.

3.1.2 Natureza Jurídica

O nosso objetivo neste capítulo passa por explorar as principais normas que regulam a prova digital para enquadramento legal, não sendo uma análise extensa das mesmas uma preocupação no presente trabalho. São elas o CPP; a Lei n.º 109/2009 de 15 de setembro; Convenção sobre Cibercrime; Lei n.º 32/2008, de 17 de julho; Lei nº 41/2004, de 18 de agosto e Regulamento (UE) n.º 910/2014 de 23 de julho; Regulamento Geral sobre a Proteção de Dados, de 2018.

No CPP, as disposições relativas à prova digital, no que concerne à obtenção do meio de prova, encontram-se explanadas nos art(s). 189º e 190º nos quais não consta um regime legal específico relativo à prova digital, mas antes uma alusão aos art(s) 187º e 188º do mesmo diploma. Isto é, a todas as conversações ou comunicações transmitidas por meio de suporte eletrónico diferenciado do telefone (*e.g.* correio eletrónico) é-lhes atribuída a mesma admissibilidade, requisitos e pressupostos das interseções das escutas telefónicas.

Nas palavras de Almeida (2014), fala-se na inexistência de um regime jurídico relativo à prova digital, no sentido especificado. Ou seja, os meios de prova colhidos em ambiente digital embora tipificados no CPP, não encontram uma referência concreta à prova digital. E para além do exemplo acima descrito, em sede de obtenção de prova, uma dessas situações é espelhada no art. 179º do CPP, respeitante às apreensões, podendo o juiz "autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência", permanecendo no vazio jurídico o que se entende por "qualquer outra correspondência", não sendo especificada a "correspondência eletrónica" (Almeida, 2014).

É igualmente importante comentar a Lei n.º 109/2009, de 15 de setembro, ou Lei da Cibercriminalidade, que transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, referente a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Nela estão delimitados vários conceitos essenciais ao domínio da criminalidade informática (art. 2º), a tipificação dos seus crimes (art. 3º a 10º) e várias disposições relativas à recolha de prova em suporte eletrónico. Este diploma, confere, com efeito, "[...] um complexo normativo processual penal relativo à recolha de prova digital com remetente a um universo de crimes distintos" (Costa, 2017, p. 87), introduzindo novos meios de investigação e produção de prova próprios ao combate à criminalidade informática.

A Convenção sobre Cibercrime do Conselho da Europa (2001), supramencionada, ou Convenção de Budapeste, aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, foi o primeiro tratado internacional a lidar com a internet e a criminalidade no Ciberespaço e teve como principal finalidade o acompanhamento e harmonização dos elementos relativos às infrações do direito penal - respeitantes a crimes realizados através de meios eletrónicos, ou seja, a Cibercriminalidade - entre os países signatários.

Para o efeito, é vital a referência à Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, onde são estabelecidas as regras relativas à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Recentemente, em abril de 2022, a também conhecida por Lei dos Metadados, viu alguns dos seus artigos declarados inconstitucionais pelo TC que regulavam as categorias de dados a conservar, o período de conservação e a transmissão desses dados às autoridades, presentes nos art(s) 4º, 6º e 9º, respetivamente. Através do Acórdão n.º 268/2022, o TC considerou que tais normas violavam direitos e princípios consagrados na Constituição, nomeadamente o princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar ou o sigilo das comunicações. Porém, dada a relevância do tema e as potenciais consequências para efeitos de investigação criminal, o Governo apresentou uma proposta de lei (Proposta de Lei nº11/XV/1ª), que permitisse de igual modo dotar as autoridades competentes dos meios de obtenção de prova necessários à investigação de tais crimes, aprovada em maio do ano passado.

Outros documentos relevantes dizem respeito ao Regulamento Geral sobre a Proteção de Dados, aplicável desde Maio de 2018, é o novo regulamento que revoga a Diretiva de Proteção de Dados de 1995 (Diretiva n.º 95/46/CE) e substitui a Lei nº 67/98 de 26 de outubro, relativamente à proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação desses dados, imprescindível no domínio da prova em meio digital. De modo a especificar e complementar a mesma, foi criada a Lei nº 41/2004, de 18 de agosto, que transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, aplicada ao tratamento de dados pessoais no contexto das redes e serviços de comunicações eletrónicas acessíveis ao público.

Por fim, o Regulamento (UE) n.º 910/2014, de 23 de julho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno,

diretamente aplicável em toda a Europa, sem necessidade de transposição para a legislação interna.

Após esta breve análise às principais normas que regulam a prova digital, conclui-se que é uma preocupação europeia, sobretudo desde o ano de 2001, integrar o contexto da prova digital ao meio legal, através da adoção de Decisões, Convenções, Diretivas e outros atos legislativos. Este facto é justificado pela ascendência do digital sobre as nossas vidas, que deve ser acompanhado de um quadro jurídico o mais sólido quanto possível.

3.1.3 Dificuldades colocadas pela sua natureza

Como previamente discutido, os benefícios da prova digital para a descoberta da verdade material na concretização da justiça são incontestáveis. Porém, a par da sua utilidade, a prova digital é também acompanhada de inúmeras dificuldades que arrastam consigo uma infinidade de especificidades a ter em conta quando dela se trata. Iniciamos este tema apresentando os principais constrangimentos deste meio de prova alusivo às buscas, apreensão, aquisição, análise e tratamento desta.

Efetivamente, é necessário considerar que a presença de prova digital e a respetiva obtenção não ocorrem nos mesmos moldes que a prova física de qualquer outro crime, seja ela a apreensão de uma carta ou um outro qualquer documento, por exemplo, jamais oferecendo o mesmo conforto dos anos de prática com que são encarados os métodos e meios de prova clássicos (Costa, 2017). Sendo a prova digital consequência direta de um mundo abstrato de natureza tão particular, esta "imaterialidade" pelo qual é revestida gera, desde logo, adversidades na identificação do agente e local onde é cometido o crime face ao anonimato oferecido pelas TIC, como aprofundado no capítulo 1. Tonini (2010) explica que, enquanto a prova material se incorpora em suporte físico, a prova digital, embora careça de uma representação física em suporte material, não se resume a nenhum deles. A sua complexidade e codificação exige, assim, conhecimentos técnicos específicos por parte dos investigadores e peritos digitais forenses, necessários à boa operação da prova sob pena de se perder a sua força.

Normalmente, a identificação do dispositivo pela qual se procede a uma ação criminosa é possível através do endereço IP[27] bem como o endereço MAC[28], porém, urge a dificuldade de

[27] O endereço IP, do inglês *Internet Protocol*, refere-se à identificação de um dispositivo (smartphone, computador, etc.), representada por números, conectado a uma rede local ou pública ou à internet. Serve, sobretudo, dois propósitos possíveis: identificação de interface de utilizador ou de rede e endereço de localização.

[28] O endereço MAC, do inglês *Media Access Control*, é um código único que identifica a placa de rede de determinado dispositivo (também presente em smartphones, computadores, etc.) composto por doze dígitos, permitindo uma

determinar a pessoa que fez uso da tecnologia de informação visto que os mesmos nada revelam sobre o seu utilizador. Contrariamente à criminalidade tradicional, no Ciberespaço, a autenticação dessa identidade geralmente apresenta um maior número de limitações face à impossibilidade de "[…] verificação de documentos ou de elementos identificadores já em si evidentes" (Aras, 2015, p. 37) por exemplo, a recolha de vestígios físicos ou a existência de testemunhas oculares. A isto soma-se a possibilidade do agente do crime se revestir de uma identidade virtual, ou mesmo de terceiros, o que poderá condicionar a investigação. Esta panóplia de fatores torna a relação entre o crime e a ação do agente que o cometeu, no mínimo, complexa.

E é facto que na maior parte dos casos, esta prova "[...] raramente se encontra exactamente no local do crime" (Almeida, 2014, p. 32), bem como a deslocação física não se impõe em todos os casos fruto da sua natureza remota, que de igual forma a ela se pode aceder (Ramos, 2014). A somar, está a dificuldade em determinar o momento e data do mesmo, em razão da simplicidade em alterar datas e horas, prejudicando a investigação. Isto é, qualquer informação identificativa vê a sua valoração mitigada em razão da facilidade de alteração de qualquer tipo de indício probatório, sendo esta uma das variadas razões para aferir a fragilidade da prova digital, a que se refere Rodrigues (2009).

Assim, em resultado da sua alterabilidade, "[...] carece de ser tratada de forma diferente, digamos que de modo delicado" (Ramos, 2014, p. 87) pois a sua manipulação descuidada pode traduzir-se na alteração das suas propriedades – ou até no seu desaparecimento - e com isso se perca a integridade da prova. A título de exemplo, abrir um documento ou clicar numa tecla é o suficiente para a sua adulteração. Por essa razão a produção de prova tem protocolos e regras específicas para manter a cadeia de custódia da prova, um dos pilares fundamentais neste tipo de obtenção probatória, tema aprofundado no subcapítulo que se segue.

Outrora, é também imprescindível mencionar que as vulnerabilidades apresentadas, nomeadamente no que diz respeito à fragilidade da prova, pode também ela representar uma força. Apesar da possibilidade de eliminação de ficheiros e dados, e assim contaminar a prova, a taxa de sucesso por parte da equipa de peritos forenses na recuperação dos mesmos é ainda elevada. Consequentemente, faz-se questionar o motivo pela qual houve tentativa de adulteração dos dados, válido, em parte, para formar a convicção do tribunal.

infinidade de combinações e, consequentemente, a respetiva exclusividade. Distingue-se do endereço IP – dinâmico e passível de alterar-se com o tempo - por ser fixo, exclusivo e mais preciso na identificação do dispositivo em causa. Porém, e mesmo assim, é suscetível de adulteração.

Conclui-se que, fruto da sua genética, identifica-se um caráter dinâmico, instável e volátil, personalidade que dificulta tanto a perícia forense como a investigação. É imprescindível, assim, a rapidez na sua obtenção juntamente com uma recolha de prova devidamente apropriada tanto para a imputação dos factos como para inocentar o arguido e assegurar, consequentemente, a descoberta da verdade.

3.2. Cadeia de custódia da prova

Tendo em conta as dificuldades apresentadas pela prova digital, é fulcral garantir um conjunto de metodologias e procedimentos de modo a assegurar a integridade da mesma e, assim, potenciar a condenação dos que se dedicam a práticas criminosas como a exploração sexual de menores no Ciberespaço. Conforme refere Rodrigues (2011, p. 47), "[…] a prova electrónico-digital somente será válida, num dado processo penal, se forem respeitadas as várias regras ao nível do seu acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição". Neste sentido, é imprescindível explorar a "cadeia de custódia da prova" ou a também identificada como "cadeia probatória" da prova digital.

O ordenamento jurídico português não prevê a sua definição, embora possam ser apresentadas referências doutrinárias consideradas relevantes para uma leitura percetível do tema. Prado (2021) define-a como um "[…] método por meio do qual se pretende preservar a integridade do elemento probatório e assegurar sua autenticidade". Por sua vez, na senda de Magriço (2012, p. 49) refere-se à "[...] capacidade de garantir a identidade e integridade de um espécime ou amostra no decurso da sua obtenção (*e.g.* numa busca), durante a sua análise e até ao final do processo". Acrescenta ainda que "consiste em salvaguardar e proteger a informação digital apreendida, de forma documentada, de modo que não possa alegar-se que foi modificada ou alterada durante a IC." (Magriço, 2012, p. 49).

Valente (2019, p. 45) diz-nos, mais pormenorizadamente, que a cadeia de custódia é "[...] uma técnica jurídico processual que garante a identidade e autenticidade da prova ab initio ad finem de todo o *iter processualis* – desde o meio de obtenção da prova (busca e apreensão), a submissão a meio de prova (perícia) que termina a ser submetida à apreciação do Tribunal e ao contraditório, próprio das jurisdições processuais de estrutura acusatória (prova como resultado)".

A relevância da prova digital é indubitável, outrora, para além de carecer de concetualização legal, não estão também positivados os procedimentos a adotar pelos

responsáveis na recolha, aquisição e análise da mesma no ordenamento jurídico português. Este apenas oferece no art. 249º, nº2, alínea a), do CPP, que compete aos OPC "proceder a exames dos vestígios do crime [...] assegurando a manutenção do estado das coisas, dos objetos e dos lugares", isto é, garantir a cadeia de custódia. Este facto contraria países como Chile, Colômbia, Equador e Perú, por exemplo, que que adotam um manual de procedimentos para a regulamentação legal da cadeia probatória (Hermeiro, 2023), assim como o Brasil que no art. 158 do seu CPP, define cadeia de custódia bem como as etapas a respeitar na sua manutenção.

Porém, apesar deste "vazio" em Portugal, seguem-se algumas recomendações de boas práticas, das quais destaco a Norma ISO/IEC 27037 de 15 de novembro de 2012, o NIST – *Best Practice manuals,* o *Electronic Evidence Guide – A basic guide for police officers, prosecutors and judges* do Conselho da Europa e o ENFSI-BPM-FIT-01 (2015) da Rede Europeia de Institutos de Ciências Forenses. Para o efeito, podem ser igualmente mencionados organismos internacionais que deram o seu contributo nesta matéria, nomeadamente o *Scientific Working Group on Digital Evidence* (SWGDE), *Association of Chief Police Officers* (ACPO) e *International Organization on Computer Evidence* (IOCE).

Ora, antes de explorarmos, de facto, os procedimentos de recolha de prova digital, cabe-nos considerar que a sua obtenção deverá respeitar um conjunto de princípios gerais orientadores tendo como referência a *International Hi-Tech Crime and Forensics Conference*[29] de 1999, e, tratando-se de um trabalho de investigação que alude ao trabalho da Polícia de Segurança Pública nesta matéria, o Manual Técnico de Preservação e Recolha da Prova digital na Investigação Criminal (2015) da PSP, fulcrais para se preservar a cadeia de prova.

Desde logo, qualquer procedimento inicial deverá ser realizado por uma equipa de pelo menos duas pessoas com conhecimentos técnicos e com recurso a ferramentas adequadas, e assim assegurar o princípio da responsabilização repartida dos vários intervenientes na produção da prova. Este confere-lhe maior proteção jurídico-legal bem como se permite uma maior eficácia na sua recolha.

Em segundo lugar, um dos princípios indispensáveis a respeitar é o de não alteração da prova no seu tratamento. Como supramencionado, a prova digital é "frágil" e em razão da sua personalidade será exigido que quer o investigador quer o perito digital excluam da sua conduta, durante o decorrer da investigação e da perícia, qualquer atuação que possa contaminar os

[29] FBI. (2000). Digital Evidence: Standards and Principles. *Forensic Science Communications, 2*(2). https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

dados obtidos. Afinal, uma prova não possui valor algum se não for comprovadamente íntegra[30] e autêntica[31]. A mencionar, a título de exemplo, a função *hash*[32], um algoritmo que gera um código de identificação exclusivo - código hash[33] - de um ficheiro ou um conjunto de ficheiros. Isto é, se a prova digital for de alguma maneira alterada de, o algoritmo irá produzir um código diferente quando comparada ao original[34], sendo este o motivo pela qual é utilizado como confirmação da inalterabilidade da prova durante o decorrer do processo-crime. Equipara-se, segundo Magriço (2012, p. 60), ao DNA digital, "na medida em que é univocamente identificada uma determinada informação de carácter digital".

Logicamente, a sua autenticidade apenas será concretizável com recurso a um terceiro princípio: o registo da cadeia da prova. Por outras palavras, deverá proceder-se à documentação dos procedimentos executados na interação com os sistemas informáticos[35] em todas as fases processuais (o acesso, recolha, armazenamento, transferência, preservação e apresentação da prova digital). Este registo deverá conter, entre outras, as seguintes informações: registo identificador único de prova; registo de quem acedeu à prova digital, data, hora e local em que ocorreu; registo de quem e quando foi verificada a prova digital dentro e fora das instalações de armazenamento; registo de acesso às provas (o seu propósito) e da autoridade competente, se for o caso (ISO, 2012). No Anexo A é disponibilizado, a título de exemplo, o modelo de cadeia de custódia em uso da Polícia de Segurança Pública.

[30] Integridade, de acordo com o dicionário enciclopédico online da Porto Editora, refere-se ao "estado ou qualidade do que se mantém intacto ou inteiro". No presente contexto, pressupõe que se garanta, no ato de apreensão e aquisição dos dados informáticos do sistema informático, a não alteração da prova. De referir que, no documento ISO (2012, p. 10), a integridade da prova é definida como a "[...] propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental".

[31] A autenticidade a que aludimos refere-se à capacidade de confirmar a integridade dos dados informáticos. A cadeia de custódia desde a cena do crime até à pesquisa informática e, finalmente, até ao tribunal, na forma de uma trilha de auditoria, é uma parte importante do estabelecimento da autenticidade da prova digital.

[32] Numa das versões do código hash (MD5) foi verificada que a possibilidade de dois ficheiros distintos terem o mesmo código, tornando esta opção pouco viável para garantir a exclusividade de cada ficheiro. Assim, é imprescindível a utilização de dois códigos hash na sua validação ou, ao usar-se apenas um, optar pelo SAH-256 ou mais forte.

[33] O código hash resulta da "[...] transformação de uma grande quantidade de informações (informação original) em uma pequena sequência de bits (valor hash)" (Eleutério & Machado, 2014, p. 128).

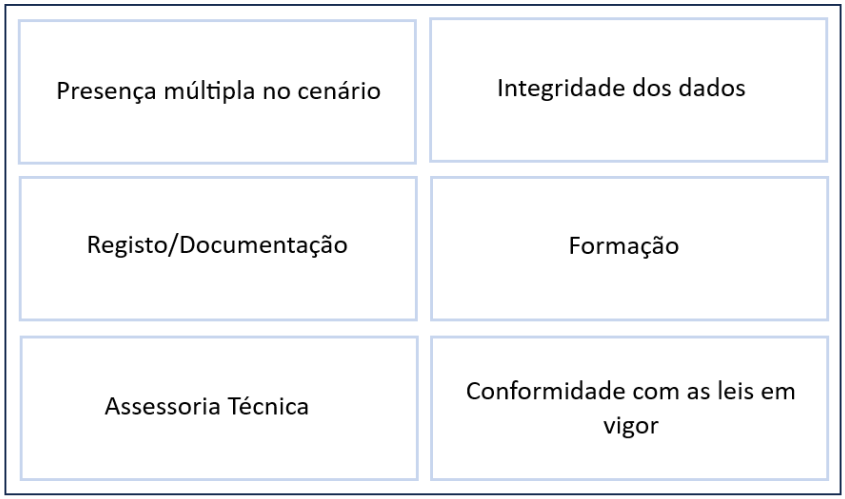
[34] Tem-se como original o código gerado no momento em que o dispositivo é apreendido.

[35] De acordo com a Lei do Cibercrime, art. 2º, alínea a), tem-se como sistema informático "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção". De modo corriqueiro, poderá desginar-se igualmente por equipamento eletrónico.

Seguidamente, o princípio da especialização ou qualificação de todos os intervenientes num processo de investigação criminal nomeadamente *first responders*[36], investigadores, peritos informáticos forenses e magistrados judiciais e do ministério público, que os dotem de capacidades e competências técnicas específicas. A par desta, a assessoria técnica, ou seja, no âmbito de uma operação onde é previsível a recolha de prova digital deve ser garantida atempadamente a presença de um perito informático forense, nomeado por despacho da autoridade judiciária conforme disposto no art. 154º do CPP.

Por fim, o dever de conformidade com as normas legais em vigor, nomeadamente quanto à proteção dos dados pessoais, ao segredo profissional e aos dados clínicos, bancários, de comunicação e outros especificados na lei, que deverão ser estritamente cumpridas por todos os elementos intervenientes aos quais é exigida responsabilidade pessoal no controlo da cadeia de custódia. A Figura 5 permite uma visão mais esquematizada sobre a panóplia de princípios referidos.

Figura 5. Princípios inerentes à cadeia de custódia da prova



No presente subcapítulo é de referir ainda um ponto bastante pertinente respeitante à livre apreciação da prova. Este princípio determina, sucintamente, que a prova apresentada é sujeita à livre apreciação do juiz, que lhe confere força em função da sua experiência e livre convicção, conforme disposto no art. 127º do CPP, necessariamente objetiva e imparcial. Porém,

[36] Expressão em inglês para se referir a um técnico de primeira resposta, isto é, aquele que dispõe do primeiro contacto com os sistemas informáticos e que pode não ser perito na matéria em questão.

a prova pericial – e, para o efeito, a prova digital - encontra-se subtraída à livre apreciação do julgador (art.º 163º, nº1 do CPP), que ao ver cumpridos todos os princípios da legalidade inerentes ao seu tratamento, é considerada um tipo de prova quase[37] indubitável.

Por outro lado, a quebra na cadeia de custódia resultará numa "[...] proibição total de admissibilidade e de valoração da prova por se terem violado regras processuais tão importantes, assim como direitos fundamentais" (Hermeiro, p. 43, 2023), num total prejuízo para a obtenção da verdade. Por outras palavras, é um processo irreversível que não oferece outra possibilidade senão a sua invalidade, impedindo que se absolvam os culpados e se condenem os inocentes.

3.3. Procedimentos e boas práticas para tratamento da prova digital

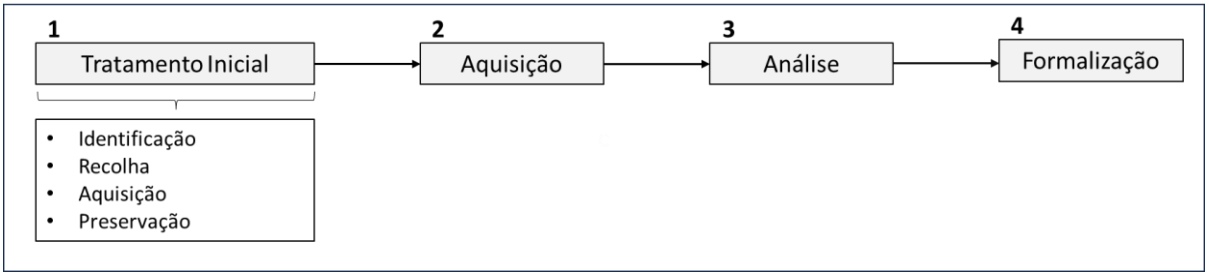
3.3.1 Tratamento inicial

Os modelos de recolha de prova digital são variados, contendo um número, sequência e classificação diferenciado de etapas consoante o autor ou organização que as estabelece, variando o procedimento específico de acordo com o tipo de incidente ou o caso que esteja sob investigação. Todavia, na presente dissertação, concentraremos a nossa atenção especialmente nas recomendações da ISO (2012) em consonância com o estabelecido no ordenamento jurídico português, complementando a mesma com recurso a alguns documentos e autores considerados relevantes.

Com base no descrito nesta Norma, e por forma a estruturar o raciocínio sobre o tema, é possível desenhar um quadro que permita melhor identificar as etapas necessárias ao tratamento da prova (Figura 6).

[37] Considera-se "quase" indubitável face à possibilidade de pedido de contraprova por parte do tribunal, se assim for justificado.

Figura 6. Principais fases do processo de análise digital forense



Embora o processo completo de tratamento de prova digital inclua outras atividades, o âmbito desta Norma refere-se apenas ao processo de tratamento inicial que consiste na identificação, recolha, aquisição e preservação de potenciais Provas Digitais (ISO, 2012), objeto de análise numa primeira instância. Focar-nos-emos, neste subcapítulo, nos procedimentos a adotar no tratamento inicial da prova pelos *first responders*.

Primeiramente, o processo de identificação da prova digital, de acordo com a ISO (2012) envolve a busca, reconhecimento e a documentação da mesma.

As buscas são instrumentos (meios de obtenção de prova) de que se servem as autoridades judiciárias para recolha de informação relativamente a um ou mais crimes. Segundo o nº 1 e 2, do art. 174.º do CPP, é ordenada busca quando houver indícios de que existam animais, as coisas ou objetos, em local reservado ou não livremente acessível ao público, relacionados com o crime ou que possam servir de prova. A competência para ordenar busca pertence à autoridade judiciária competente, nos termos do art. 174.º, n.º 3 do CPP, à exceção dos casos previsto no art. 174.º, n.º 5 do mesmo diploma, que regula os casos em que os órgãos de polícia criminal podem efetuar buscas por iniciativa própria.

Chegados ao local da busca, antes da apreensão da prova, será imprescindível efetuar-se a uma série de procedimentos operacionais que impeçam a contaminação do local, como nos casos que envolvam a exploração sexual de menores no Ciberespaço. No âmbito de uma operação de busca, indicam-se brevemente alguns passos a seguir em conformidade com o Manual Técnico de Preservação e Recolha da Prova Digital na Investigação Criminal da Polícia de Segurança Pública:

- Afastar todas as pessoas dos sistemas informáticos a analisar;
- Não permitir que alguém (especialmente o suspeito) toque no teclado ou rato face à possibilidade de destruição da prova;

- Considerar eventuais acessos remotos aos sistemas, nomeadamente dispositivos com capacidade de acesso sem fios, através da rede interna ou através de um acesso por rede externa (internet);
- Possuir equipamento de proteção adequado.

Soma-se ainda, segundo a ISO 233705 (2012), a procura por elementos como *post-its*, diários, papéis, *notebooks* ou manuais de *hardware* e *software* que possam conter informações cruciais sobre os dispositivos, como senhas e PINs, quando e se permitido.

No decorrer desta primeira etapa devem ser identificados e selecionados um número máximo de sistemas informáticos, os quais possam conter dados informáticos relevantes para o processo-crime em investigação, e assim, ser utilizados como prova. Este procedimento deverá ser adequado ao crime em questão – não devendo ser apreendido qualquer dispositivo apenas por se encontrar no local da busca - cuja decisão cabe ao chefe de equipa ou responsável pela coordenação da operação. Selecionar o que é relevante é o desafio das fases de **reconhecimento** e recolha, porém, sob condições desfavoráveis, considera-se preferível recolher a maior quantidade possível de provas para posterior seleção na fase subsequente da investigação. Não obstante, é também fundamental priorizar-se a recolha com base na alterabilidade da prova, aplicável se as circunstâncias específicas do caso a ser investigado assim o exigirem. Isto significa que deverá iniciar-se a apreensão dos sistemas informáticos mais voláteis (*e.g.*, RAM[38]) para os menos voláteis (*e.g.*, disco rígido[39]). Esta priorização por grau de relevância é um dos desafios encontrados pelos *first responders* que se torna mais eficiente e efetiva quando ocorre no local, onde as potenciais provas se encontram no contexto em que foram produzidas. Verificar se será relevante a recolha de outro tipo de vestígios (*e.g.* biológicos, lofoscópicos, produto estupefaciente) e, se assim exigido, chamar ao local outros elementos técnicos, é igualmente fulcral.

Acrescenta-se ainda que nem todos os tipos de suporte de armazenamento digital podem ser facilmente identificados e localizados, por exemplo, a computação em nuvem e NAS[40] - face à componente virtual que acrescentam ao processo de identificação - bem como

[38] Acrónimo de *Random Access Memory* que, segundo Marques (2013, p. 173) denomina "[...] o local onde o computador quando ligado coloca o sistema operativo, os programas que está a executar e os dados com que está a trabalhar. É a memória de acesso mais rápido, no entanto é volátil, isto é, uma vez desligado o computador esta perda toda a informação".

[39] "É uma caixa selada, que contem os discos magnéticos que armazenam dados. Podem ser internos ou externos ao Computador" (Marques, p. 158).

[40] *Network Attached Storage,* que designa um computador ou sistema de armazenamento conectado a uma ou mais redes locais que armazena, compartilha e gera cópias de dados. (SNIA, 2023)

dispositivos que em função do seu tamanho e aspeto possam ser esquecidos ou confundidos com outro material irrelevante.

Por sua vez, deverá proceder-se à documentação de todas as atividades (seja através de registo fotográfico ou vídeo do aspeto exterior do(s) equipamento(s) e do local), como anteriormente mencionado, que apesar de se iniciar na fase de identificação, acompanha todas as etapas da cadeia de custódia. Primeiramente, é imperativo produzir-se um registo objetivo e permanente do local, das evidências materiais e de quaisquer alterações que ocorram, bem como deverão ser tidos em conta um conjunto de outros aspetos fundamentais, expostos com maior detalhe na cláusula de gestão de documentos e a cláusula de gestão de registos da norma ISO (2005).

Uma vez identificados os sistemas informáticos e dados potencialmente relevantes para a descoberta da verdade, segue-se a próxima etapa: a recolha. Será necessário aqui balizar que a busca de onde resulte uma apreensão é regulada pelas normas do CPP (constante no Cap. III, Título III sob epígrafe "Dos meios de obtenção da prova", Livro III "Da prova"), porém, a pesquisa de dados de um sistema informático, bem como a sua apreensão, estão regulados na Lei do Cibercrime. Nesta fase, segundo os pressupostos dispostos do art. 16º, nº1, da respetiva Lei, "Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos". O OPC pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do art. 15º da LC, bem como quando haja urgência ou perigo na demora (art. 16º, nº2), porém, as mesmas estão sujeitas à validação pela autoridade judiciária competente no prazo máximo de 72 horas (art. 16º, nº4).

Segundo o Manual da PSP[41],considera-se a existência de dois métodos genéricos de recolha da prova digital, cuja aplicação varia consoante as circunstâncias que melhor se adequam ao caso concreto: recolha do suporte digital ou recolha direta da informação contida no suporte digital. O primeiro, constante no art. 16º, nº7, alínea a), da Lei do Cibercrime ("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") refere-se à recolha física do sistema informático que possa conter prova digital,

[41] Manual Técnico de Preservação e Recolha da Prova Digital na Investigação Criminal (2015)

removido do seu local original para um laboratório ou outro ambiente controlado para posterior aquisição[42] e análise. O leque dos dispositivos que se podem apreender são inúmeros, por exemplo, computadores, outros dispositivos eletrónicos e dispositivos de armazenamento (Apêndice A). O segundo método refere-se à aquisição de dados dos sistemas informáticos diretamente no local de busca, especificamente indicado para situações em que seria inconcebível apreender dezenas de computadores, não sendo viável a sua recolha, ou em situações que possam representar grave prejuízo para o funcionamento de um local de trabalho (no caso de apreensões realizadas em escritórios empresariais, *e.g.*). Este tipo de recolha exige ferramentas forenses particulares, sendo quase forçosa a presença e a sua execução por pessoal qualificado ou familiarizado com este tipo de meios. No subcapítulo seguinte serão abordadas outras particularidades relativas à aquisição de dados.

São ainda indicadas algumas vantagens e riscos associados a cada um dos respetivos métodos de recolha no Apêndice B.

Em razão do até então descrito, a preservação da prova é um dos pontos essenciais a assegurar durante todas as etapas, podendo ser definida como a capacidade de garantir que a informação digital se mantém acessível e autêntica para que possa ser devidamente interpretada no futuro, com recurso a uma plataforma tecnológica distinta da utilizada no momento da sua criação (Ferreira, 2006). A ação de etiquetar, embalar e selar, ou de acordo com Marques (2013), "Bag&Tag", correspondente à denominação anglo-saxónica, representa uma das formas de preservação da prova. Na ISO (2012) são indicados alguns passos a cumprir, dos quais se destacam:

- Os computadores e dispositivos digitais devem ser embalados de forma a evitar danos causados por choques, vibrações, altitude elevada, calor e exposição à radiofrequência durante o transporte;
- Deve ter-se em conta a sensibilidade do dispositivo digital[43]. No que respeita à eletricidade estática, caso se verifique necessário, deverá ser acondicionado num saco anti-estático;
- Como precaução, o DEFR poderá considerar o uso de um saco *Faraday* para acondicionamento de dispositivo móvel;

[42] Segundo Antunes e Rodrigues (2022, p. 155) a aquisição "consiste em extrair os dados alojados no equipamento que está a ser alvo de perícia".

[43] "Os dispositivos digitais são frágeis e sensíveis à temperatura, à humidade, a choques, à eletricidade estática e a campos eletromagnéticos." (Magriço, 2012, p.58).

- De modo a garantir a identificação correta, é necessário rotular as possíveis Provas Digitais. A etiqueta não deve ser colocada diretamente na componente mecânica do dispositivo e não deve cobrir ou ocultar informações identificativas relevantes;
- Quando possível, os dispositivos digitais com aberturas e componentes móveis devem ser lacrados com selos de segurança apropriados. (p. 18)

No Anexo B é possível consultar um glossário gráfico que serve de ilustração de alguns materiais utilizados pela PSP para acautelar a prova digital.

Após o seu acondicionamento, procede-se ao transporte**,** que deverá ser vigiado durante todo o processo de modo a impedir alterações e, assim, manter a integridade dos dispositivos e possíveis provas digitais. De referir que qualquer pessoa que receba ou entregue um sistema informático deverá assinar um respetivo formulário, mantendo assim a cadeia de custódia.

Estas são as principais etapas descritas na ISO (2012), porém, tal como foi anteriormente referido, existe todo um trabalho posterior na aquisição de prova digital nos casos que assim o exigem. No próximo subcapítulo importa explorar os procedimentos realizados na perícia digital forense realizada pela Polícia de Segurança Pública que conduzirá a uma melhor perceção e contextualização no caso prático a explorar no capítulo 4.

3.3.2 Perícia Digital Forense: aquisição, análise e formalização

Ora, na abertura deste capítulo citamos Pimentel (2020, p. 105) que afirma que "o conhecimento científico transmitido pela atividade pericial assume primordial importância na eficiência da investigação criminal moderna" sendo esta uma peça fundamental no processo probatório, responsável por responder a perguntas como: "o quê"; "quem"; "quando", "como" e, em alguns casos, "onde" e "porquê". Este tipo de prova distingue-se essencialmente do exame pois subentende a existência de especiais conhecimentos técnicos na matéria em questão, nos termos do disposto no art. 151º do CPP. De facto, o exame é um meio de obtenção de prova mediante o qual são recolhidos vestígios que podem vir a constituir meios de prova, contrariamente à perícia que constitui um meio de prova *per si*, e resulta não de vestígios ou factos em si mesmos, mas da interpretação qualificada de instituições ou pessoas dotadas de particular conhecimento artístico, técnico ou científico da matéria em questão (peritos).

Recuando ao subcapítulo anterior e no seguimento do tratamento inicial da prova digital, será necessário prosseguir com a análise digital forense, composta pelas respetivas etapas: extração ou aquisição dos dados, análise e, por fim, formalização.

Efetivamente, após a apreensão dos suportes digitais, é realizada a perícia através da aquisição de elementos probatórios dos mesmos, que permitam sustentar uma acusação criminal (Magriço, 2012). Deste modo, a primeira fase pericial alude à aquisição dos dados que, como anteriormente referido, poderá ser realizada tanto no local da busca (*live Forensics*) como em estabelecimentos próprios (laboratórios) e ainda "sempre que a perícia recaía sobre matéria que o julgador entenda ser de especial complexidade, pode então haver lugar a vários peritos, para do relatório destes, se retirar uma maior pluralidade de resultados [...]" (Ramos, 2014, p. 17-18). É ainda possível observar no Apêndice C os possíveis dados informáticos a extrair de cada equipamento.

No que concerne à aquisição em si, não se trabalha com o dispositivo original face à possibilidade de adulteração da prova. Efetua-se, pois, através de uma cópia de dados**,** também conhecida por cópia forense**,** integral ou seletiva, para um suporte autónomo de armazenamento. A primeira relativa à cópia de todos dos dados constantes no sistema informático e a segunda uma cópia parcial dos dados que apenas se consideram relevantes para o processo. Posteriormente, e de acordo com o despacho do MP, estas poderão ser diretamente remetidas para a entidade judicial competente e por ela analisada sobre o que poderá ter valor probatório ou, por outro lado, devidamente examinada pela equipa de peritos em laboratório. O primeiro caso, apesar de desenvolvido por peritos ou *first responders*, não compõe uma perícia forense face à ausência de interpretação dos dados por parte dos mesmos.

Os sistemas informáticos dos quais são extraídas potenciais provas estão supramencionadas no subcapítulo 3.3.1, acrescentando-se ainda os veículos automóveis que possuam componente digital - nomeadamente a Unidade de Controlo Eletrónico (ECU) e *info entertainement* - de onde é possível extrair informação relevante para constituir prova. Este é um trabalho desenvolvido pela PSP, pioneiros neste domínio, em Portugal. E tal como os restantes sistemas informáticos, a aquisição dos dados neles contidos varia consoante a tecnologia neles empregue - variável dependente da marca e modelo do sistema informático -, que pode (ou não) ser suportado pelos *softwares* forenses. Cada sistema informático possui uma forma específica de armazenar os dados que poderá ser cifrada de tal forma que, consequentemente, seja impossível revertê-la e proceder-se à interpretação dos dados. Assim, sistemas mais antigos possuem maior número de fragilidades de segurança, possibilitando obter

dados indispensáveis à investigação com maior facilidade, contrariamente aos sistemas modernos com cifragens complexas e com falhas ainda desconhecidas e difíceis de contornar.

Na perícia forense digital, após a aquisição, procede-se à **análise** por critérios de pesquisa, normalmente indicados como quesitos da investigação. Por exemplo, a pesquisa por palavras-chave que incluam conteúdo pertinente para a produção de prova. Porém, para a execução desta pesquisa, usualmente denominada por triagem, é forçosa a autorização ou validação da autoridade judiciária competente, tendo em conta a legislação disponível nomeadamente os art. 15º, 16º e 17º da Lei n.º 109/2009, de 15 de setembro.

Toda a aquisição e análise é feita com recurso a *softwares* que, no caso da PSP, indicam-se os seguintes:

- *Softwares opensource* ou gratuitos: Autopsy Forensics (aquisição e análise); Magnet RAMCapture (aquisição); FTK Imager (aquisição e permite fazer alguma análise).
- *Softwares* licenciados: OpenText EnCase Forensics (análise e aquisição), Tableau TX1 (aquisição); Cellebrite Physical Analyzer e Ultra (análise); Cellebrite UFED Touch 2 (aquisição); Msab XRY (aquisição); Msab XAMN (análise).

Para aquisição de dados não presentes no dispositivo - ou seja, na *cloud* - , mas acessíveis pelo dispositivo objeto de perícia, é utilizado o *software Cellebrite Cloud Analyzer* para aquisição e análise desses conteúdos. Acrescenta-se ainda o Berla iVe para aquisição e análise de dados de veículos automóveis.

O passo final corresponde à formalização da perícia, isto é, a entrega de um relatório forense em suporte papel e junto ao respetivo processo-crime, composto por uma primeira parte contendo a descrição do material utilizado, o objeto do exame forense, as ferramentas utilizadas na intervenção técnica, e uma segunda parte composta pelas observações e ensaios realizados e conclusões, como é possível visualizar no documento em anexo (Anexo C).

Por fim, e após a execução do relatório forense, as cópias realizadas deverão ser apagadas da base de dados de modo a garantir o direito à privacidade.

No Apêndice D foi desenvolvido um fluxograma demonstrativo das principais fases do processo de análise digital forense que sintetiza o que fora demonstrado ao longo do capítulo 3.3, desde o tratamento inicial da prova à realização da perícia digital e a sua formalização.

Capítulo 4 – Simulação de investigação

4.1. A investigação criminal e a PSP: contextualização

A entrada em vigor da Lei da Organização da Investigação Criminal[44](LOIC), em 2000 impeliu alterações significativas na estrutura da Investigação Criminal, devido principalmente à transferência de competências de IC à Polícia de Segurança Pública e à Guarda Nacional Republicana (GNR). Como tal, a PSP é definida, nos termos do art. 3º, nº1, alínea c) da LOIC, como um órgão de polícia criminal de competência genérica. Ou seja, de acordo com o disposto no art. 6º do mesmo diploma, cabe à PSP a investigação de crimes "cuja competência não esteja reservada a outros órgãos de polícia criminal e ainda dos crimes cuja investigação lhes seja cometida pela autoridade judiciária competente para a direcção do processo, nos termos do artigo 8.º".

Primeiramente, e de acordo com o art. 17º da Lei n.º 53/2007, de 31 de agosto, a PSP compreende a Direção Nacional, as unidades de polícia e os estabelecimentos de ensino policial. Neste capítulo, atendamos à esfera da IC, inserida na unidade orgânica de operações e segurança da Direção Nacional da PSP (DNPSP), como ilustrado na Figura 7.

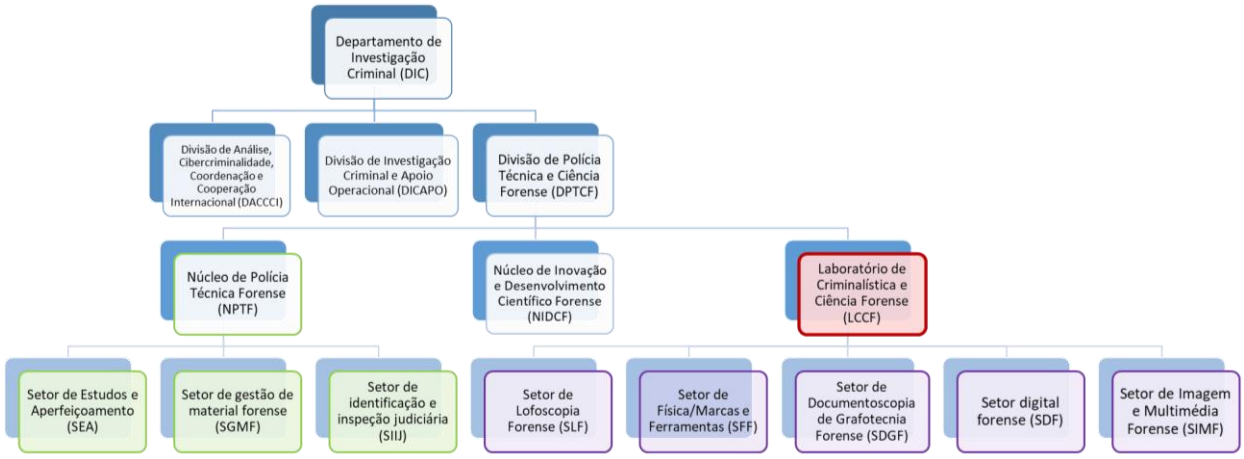
Figura 7. Organograma da Direção Nacional da Polícia de Segurança Pública

Fonte: Lei n.º 53/2007, de 31 de agosto.

[44] Lei n.º 49/2008, de 27 de agosto.

De referir a Portaria n.º 383/2008, de 29 de maio, que determinou a existência de diversas unidades nucleares da DNPSP, destacando para este estudo o Departamento de Investigação Criminal (DIC) (art. 6º). Outro diploma relevante é o Despacho n.º 19935/2008, de 28 de julho, alterado pelo Despacho n.º 6158/2017 de 13 de julho que executou acertos nas estruturas orgânicas do DIC, nomeadamente a renomeação da Divisão de Polícia Técnica e Análise Criminal (DPTAC), atualmente Divisão de Polícia Técnica e Ciências Forenses (DPTCF), que passa a ser constituída, já de acordo com o Despacho n.º 1168/2024, de 31 de janeiro, por um Núcleo de Polícia Técnica Forense (NPTF), um Núcleo de Inovação e Desenvolvimento Científico Forense (NIDCF) e um Laboratório de Criminalística e Ciência Forense (LCCF). Conclui-se que o LCCF da PSP faz parte integrante da DPTCF, pertencente ao DIC (Figura 8), sediado em Belas.

Figura 8. Organograma do Departamento de Investigação Criminal da Polícia de Segurança Pública



Fonte: Despacho n.º 1168/2024, de 31 de janeiro.

4.2. Setor Digital Forense

O Setor Digital Forense (SDF), enquadrado no Laboratório de Criminalística e Ciência Forense (LCCF) e local de realização do estágio, é composta por quatro peritos informáticos responsáveis pela realização de perícias informáticas - que se compõem na extração e análise de informação digital de sistemas informáticos - ordenadas por despacho da Autoridade Judiciária competente, ou com base nos normativos existentes neste domínio (Lei n.º 109/2009, de 15 de setembro).

O SDF tem vindo a confrontar-se com um acentuado e crescente aumento de processos-crime e realização de perícias informáticas, como constante na Tabela 4 e 5, nomeadamente entre o ano de 2019 e 2020, início da pandemia de COVID'19. Face à impossibilidade de análise de dados do Relatório atualmente mais recente (ainda por aprovar), referente ao ano de 2022, os dados apresentados remontam para o Relatório Anual da Investigação Criminal da PSP (RAIC), de 2021.

Tabela 5. Perícias realizadas pelo DIC LCCF SDF

Ano de 2021					Total
Anos de entrada	**2018**	**2019**	**2020**	**2021**	
Concluídos	7	4	51	55	117
Aguardam	0	7	24	49	80
Em execução	0	0	0	2	2

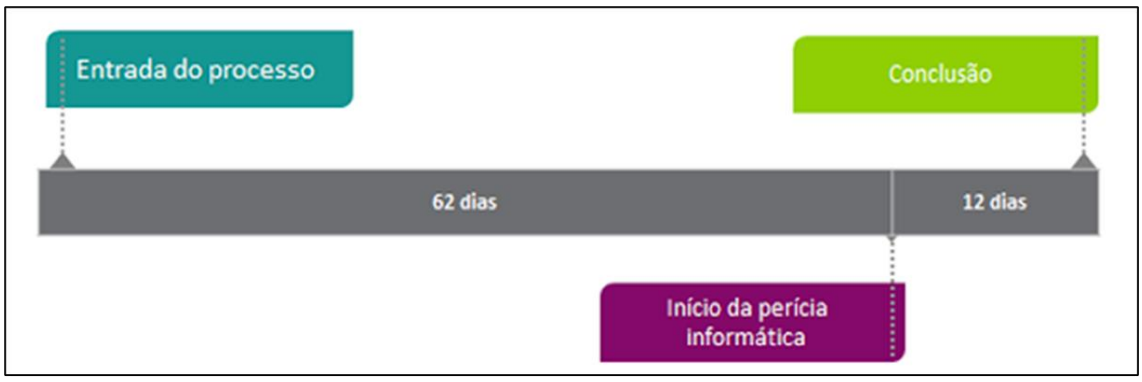
Tabela 4. Perícias realizadas pelos polos descentralizados LCCF SDF

Ano de 2021						Total
Polo	**Porto**	**Coimbra**	**Lisboa**	**Faro**	**Madeira**	
Concluídos	55	49	43	38	192	192
Aguardam	0	0	6	6	34	34
Em execução	0	0	2	2	7	7

Fonte: Adaptado de RAIC (2021).

Face à ausência de dados por tipo de crime, não nos será possível analisar as perícias alusivas ao crime contra a autodeterminação sexual de menores, porém, importa daqui retirar que o DIC LCCF SDF e os polos descentralizados se têm munido de recursos que os permitem dar resposta à evolução do número de sistemas informáticos e processos-crime remetidos para realização de perícia informática.

Figura 9. Perspetiva temporal da execução da perícia informática



Fonte: (RAIC, 2021, p. 59)

Consideramos de igual modo importante mencionar que, comparativamente a anos transatos, se verifica uma diminuição do espaço temporal entre a entrada do processo no LCCF SDF e o início da perícia informática (RAIC, 2021). Por outro lado, face à crescente complexidade dos sistemas informáticos envolvidos e do seu aumento da capacidade de armazenamento, é possível constatar um aumento dos dias de conclusão pós início da perícia, de 10 dias em 2020 para 12 dias em 2021.

4.3. Perícia Digital Forense - Métodos, Materiais e Procedimentos

A fim de compreender o cenário da perícia digital forense nos casos de ESM online, na sua íntegra, não basta apenas explorar a sua componente teórica como é fulcral uma análise sobre como, na prática, é realizado todo este trabalho. Por outras palavras, pretendemos confrontar os princípios teóricos com a realidade prática portuguesa que, face à impossibilidade de estudar um caso real, se concretizará por meio de uma simulação de investigação, respeitando as regras pela qual se rege a Polícia de Segurança Pública.

É aqui que reside, por conseguinte, a importância e pertinência do estágio curricular, que oferece o valor necessário para que a praticidade da investigação seja concretizada e, com isto, a pergunta de investigação seja devidamente respondida. Foi possível colocar perguntas, recolher ideias, observar práticas e concluir dificuldades, conversar e adquirir opinião crítica sobre determinados factos naquela que é a realidade policial, em pleno respeito pela ética da investigação. Foram assegurados os princípios definidos pelo *The European Code of Conduct for Research Integrity* (2023), nomeadamente a honestidade na condução e divulgação dos resultados da investigação, que deverá ser completa e imparcial, a integridade e rigor, através da não utilização ou ocultação de más práticas[45], e ainda o respeito por todos os intervenientes onde recai a confidencialidade na informação obtida, quando necessário.

Assim, com o objetivo de compreender a utilização e testar a eficácia das técnicas e materiais em uso da Polícia de Segurança Pública, também comuns a outros OPC, a simulação realizada exigiu a criação de duas contas de correio eletrónico e uma conta na nuvem falsas, dois cartões SIM temporários criados exclusivamente para o efeito, fotografias retiradas da internet que figuram conteúdo de ESM e troca de mensagens e e-mails entre pessoas fictícias**.** Toda a atividade realizada nos sistemas informáticos utilizados foi anotada, permitindo fazer-se uma comparação entre a mesma e a informação que foi possível extrair, e os resultados

[45] Como más práticas de investigação têm-se todas as condutas que contrariam os princípios que deverão ser assegurados na condução de uma investigação, sob pena de colocar em causa os resultados apresentados.

apresentados foram, em parte, comprovados através de registo fotográfico (em *print screen*) de modo a garantir os princípios acima apresentados.

De modo a adquirir prova digital no caso do abuso sexual de menores no Ciberespaço interessa, nomeadamente, procurar obter pesquisas realizadas na Internet, registos de acesso à Internet, os websites acedidos, os ficheiros de vídeo e/ou imagens guardadas e/ou apagadas do dispositivo movél ou na nuvem, a existência de jogos ou de material de entretenimento de menores bem como os ficheiros enviados para outros destinatários incluindo todo o tipo de conteúdo que permita confirmar ou infirmar a existência de indícios probatórios da prática deste crime. Para tal, será foco da nossa atenção o correio eletrónico[46], websites acedidos e histórico das pesquisas realizadas através dos browsers Chrome, Safari e/ou TOR, mensagens via SMS, aplicações, ficheiros contidos no sistema, nuvem e redes sociais (Whatsapp).

No presente caso prático foram utilizados dois sistemas informáticos de comunicações (um Apple IPhone 7 e um SAMSUNG Galaxy S8) e um computador (Toshiba NB305-10GB), e para extração e análise de dados, o *Cellebrite UFED Touch 2* e o *Cellebrite Physical Analyser*, respetivamente (no caso dos telemóveis) e o *Tableau TD3* e o *OpenText EnCase Forensic*, no caso do computador. O caso que pretendemos observar encontra-se retratado na caixa a seguir, idealizado de acordo com o que poderia ser uma realidade no contexto nacional atual.

Em 2024, no seguimento de uma ação encoberta de monitorização de conteúdos de ESM no Ciberespaço levada a cabo pelas Autoridades policiais portuguesas, foram detetados dispositivos móveis fisicamente localizados em território nacional (endereço IP de Portugal) responsáveis pela criação, consumo e partilha deste material, online. Após apurada a identidade de dois dos suspeitos, foram ordenadas buscas, por despacho da autoridade judiciária competente, que resultaram na apreensão de dois telemóveis (Apple IPhone 7 e um Samsung Galaxy S8) e um computador portátil (Toshiba NB305-10GB), posteriormente reencaminhados para o Setor Digital Forense do LCCF.

[46] "De forma simples e percetível, definimos correio eletrónico como um programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através das redes de informação e comunicação, independentemente do local em que estas se encontrem, sem a necessidade deste se encontrar instalado no computador". (Ramos, p.28, 2014).

4.3.1 IPhone 7

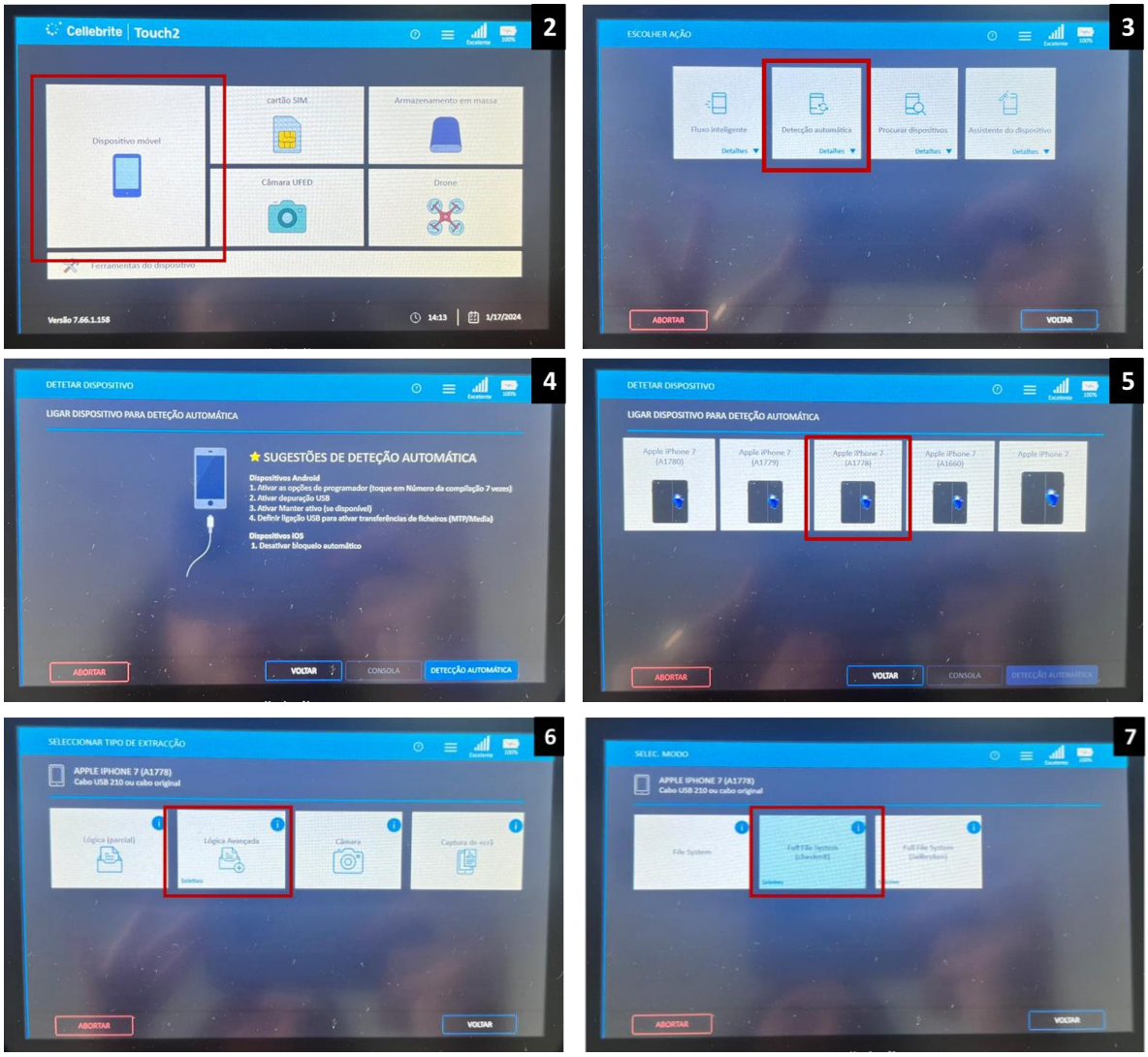
Perante o caso descrito, já em Laboratório e após preenchida a cadeia de custódia da prova (Anexo D, como exemplo meramente ilustrativo), procedeu-se à extração dos dados do IPhone 7[47], através do *hardware Cellebrite UFED Touch 2*.

Figura 10. Processo de Extração Lógica de dados do IPhone 7 (Passo 1)

Primeiramente, é necessário ligar o dispositivo móvel (neste caso, o Iphone 7) ao equipamento *Cellebrite UFED Touch 2* através de um cabo USB (Figura 10). Concretizado este passo, na tela serão exibidas várias opções relativas ao tipo de equipamento da qual se pretende extrair informação (neste caso, "Dispositivo móvel") (passo 2) precedida pela "Detenção automática" que fará a deteção quase imediata da marca e modelo do sistema informático em causa (passo 3), sendo apenas necessária selecionar o modelo específico dos cinco apresentados (A1778; passo 5).

[47] É possível consultar o registo fotográfico de ambos os telemóveis no Anexo E.

Figura 11. Processo de Extração Lógica de dados do IPhone 7



No passo 6, ser-nos-ão apresentados quatro tipos de extração pela qual é possível adquirir os dados informáticos contidos no IPhone 7, das quais destacamos:

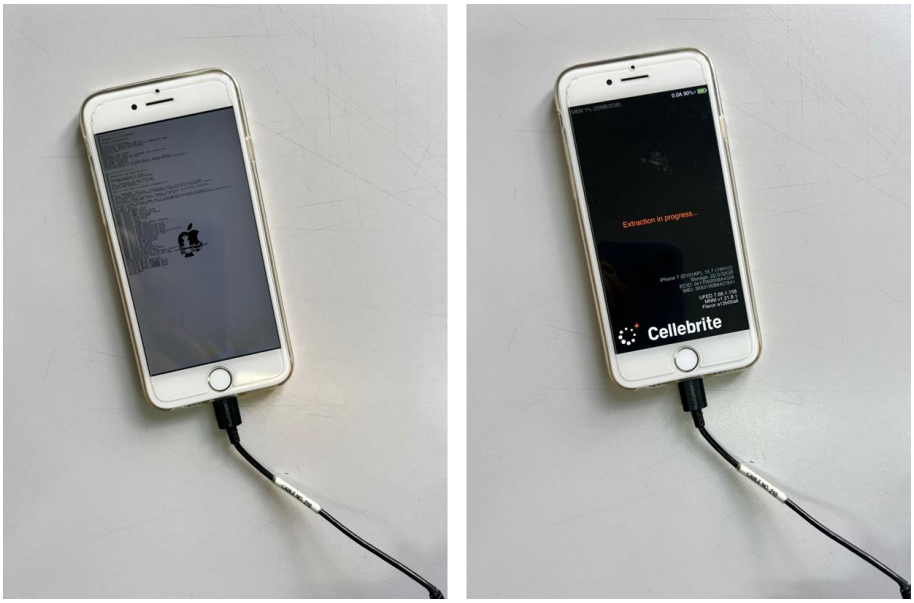
- **Extração lógica (parcial)**: um método rápido de extração que suporta o maior número de dispositivos. Os tipos de dados que podem ser extraídos incluem: registos de chamadas, listas telefónicas, SMS, eventos de calendário, ficheiros multimédia (imagens, vídeos, áudio) e dados de aplicações.
- **Extração lógica avançada:** A aquisição dos ficheiros incorporados na memória de um dispositivo móvel (o espaço alocado), incluindo imagens, vídeos, ficheiros de base de dados, ficheiros de sistema e registos. A maioria das aplicações incorporadas e do utilizador guarda os dados nestes ficheiros de base de dados. Ao efetuar uma extração do sistema de ficheiros, pode aceder-se a diversos dados, como palavras-passe, dados

de aplicações, entradas da lista telefónica, registos de chamadas, mensagens e espaço não alocado nos ficheiros.

Para o efeito, optámos pela extração lógica avançada e, posteriormente, selecionámos a opção “Full File System (checkm8)” que nos permitiu acesso a um conjunto mais alargado de dados para posterior análise.

Seguidamente, deu-se início à extração, observável na Figura 12.

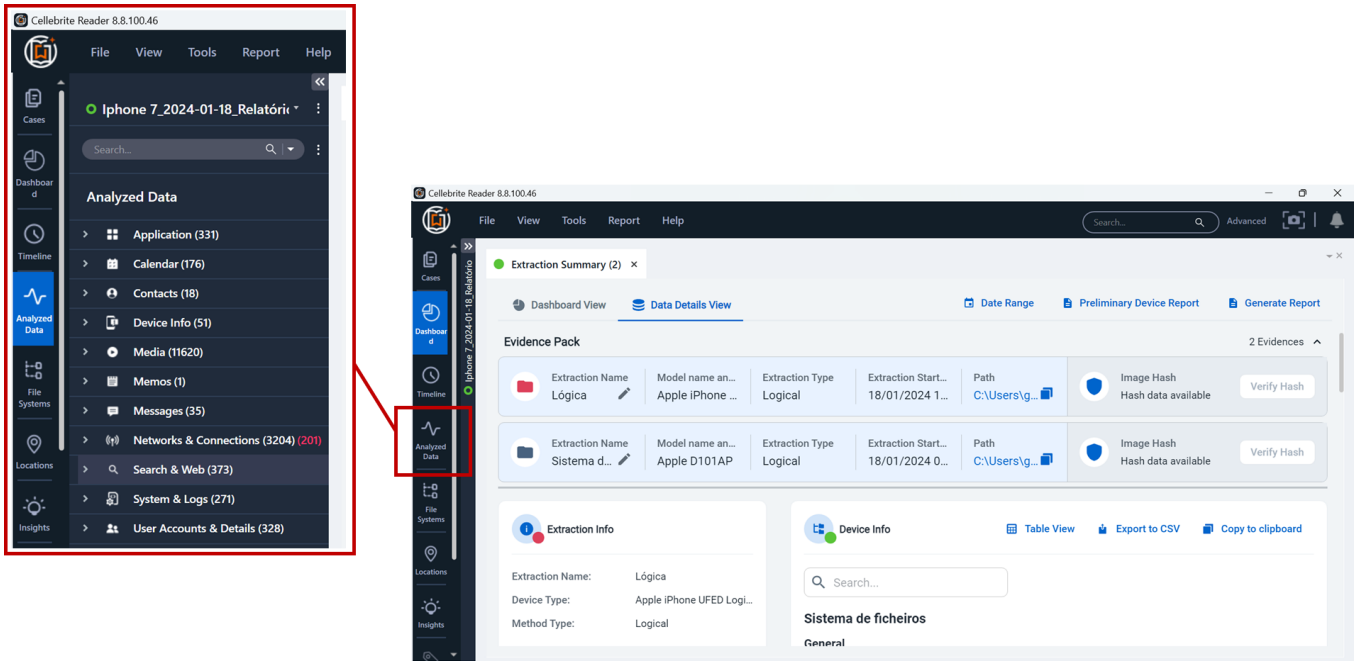
Figura 12. Início da extração lógica avançada do Iphone 7



O tempo despendido em todo este processo varia de acordo com o sistema informático apreendido e a quantidade de informação nele contido, porém, no caso referido, para extrair 32GB foram necessários 30 minutos, aproximadamente.

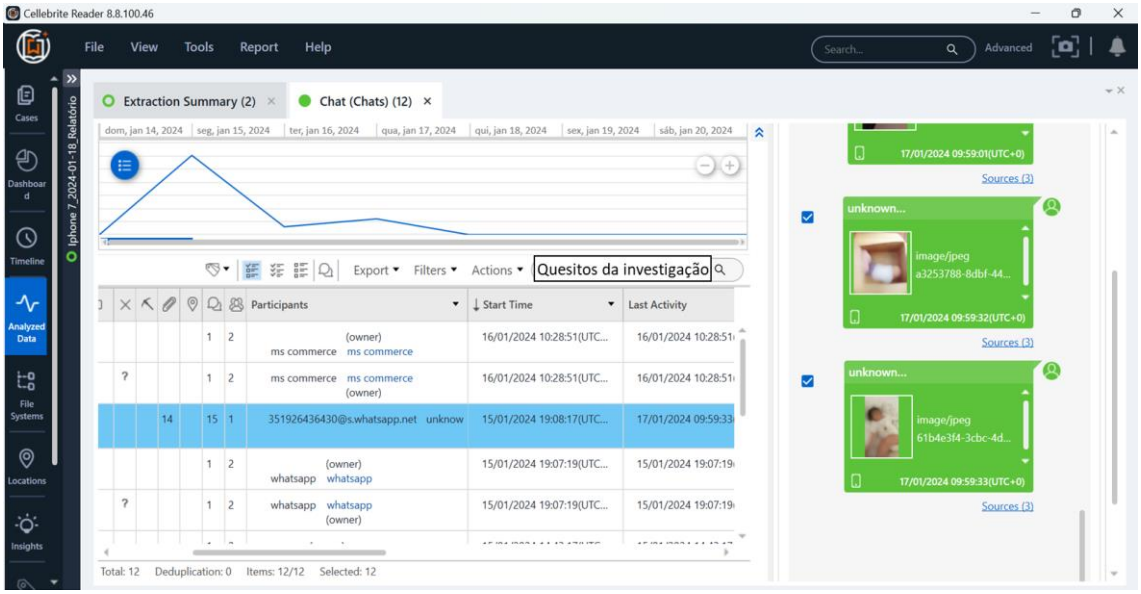
Realizada a extração, o passo seguinte será a análise da informação recolhida através do *software Cellebrite Physical Analyser.* Inicialmente, é possível argumentar sobre um conjunto de dados presentes na opção “Analyzed Data” como as aplicações, calendário, contactos, informação interna do dispositivo, fotografias, mensagens, ligações de rede, histórico da *web* e detalhes sobre o acesso e contas do utilizador. Para além do referido é ainda possível obter informações que variam desde as localizações (“Locations”), sistemas de ficheiros (“File Systems”) e o período de utilização do dispositivo (“Timeline”) (Figura 13).

Figura 13. Dados obtidos através da extração lógica



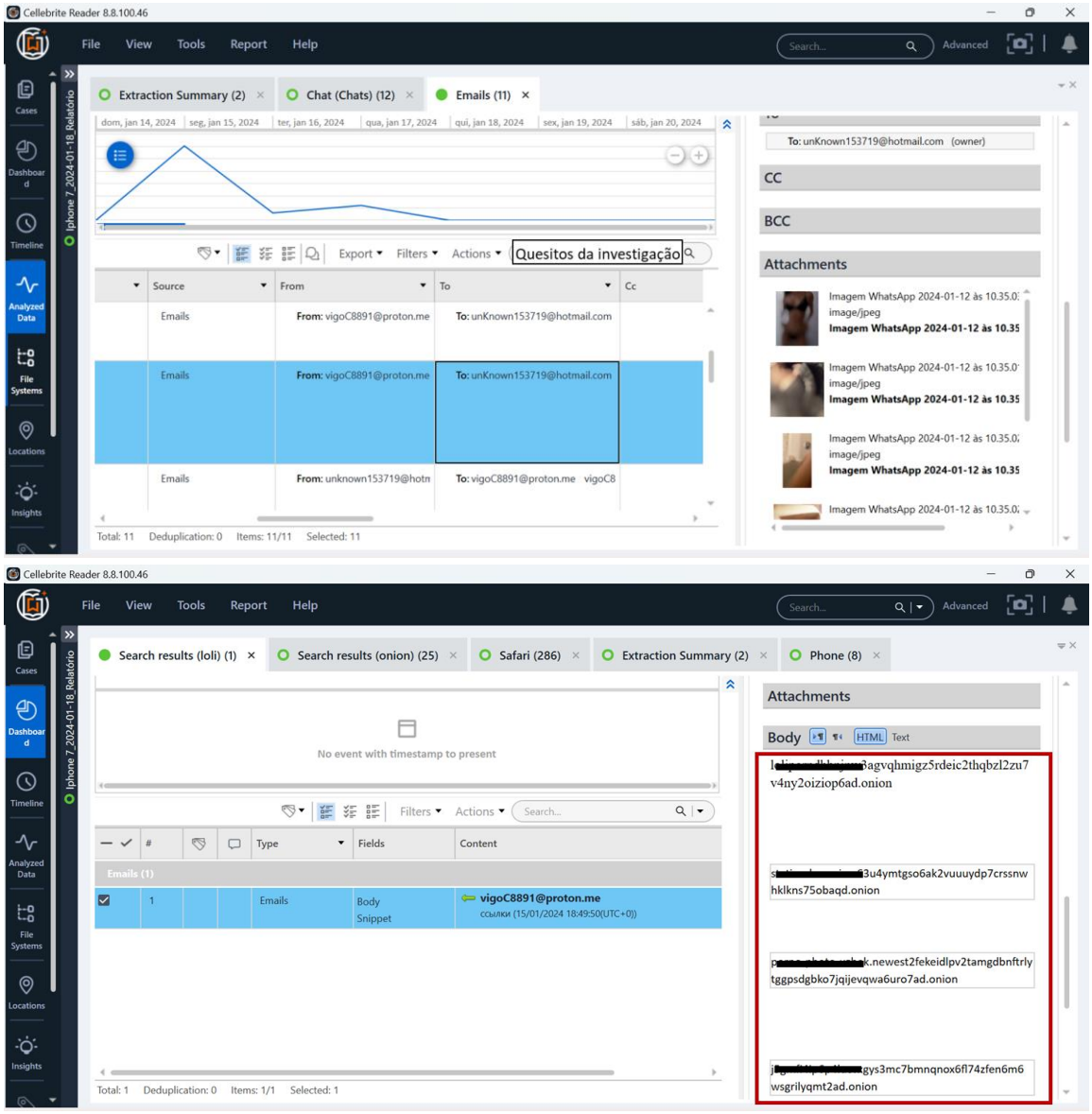
Ora, da pesquisa realizada com palavras-chaves que denunciam uma atividade de ESM (quesitos da investigação), foi encontrado conteúdo de pornografia infantil na troca de mensagens via Whatsapp. Como visível na Figura 14, é possível observar a data e hora do envio, o corpo do texto, os participantes (remetente(s) e destinatário(s)), entre outros.

Figura 14. Dados obtidos através da extração lógica (Mensagens)



Também no correio eletrónico existe a possibilidade do envio de arquivos anexados à correspondência, sendo este um dos meios utilizados pelos distribuidores de pornografia infantil para o efeito. Neste caso concreto, não só foi identificado conteúdo alusivo à ESM na troca de e-mails entre "vigoC8891@proton.me" e "unKnown153719@hotmail.com" como ainda a partilha de links *onion* que revelam sites de pornografia infantil (Figura 15).

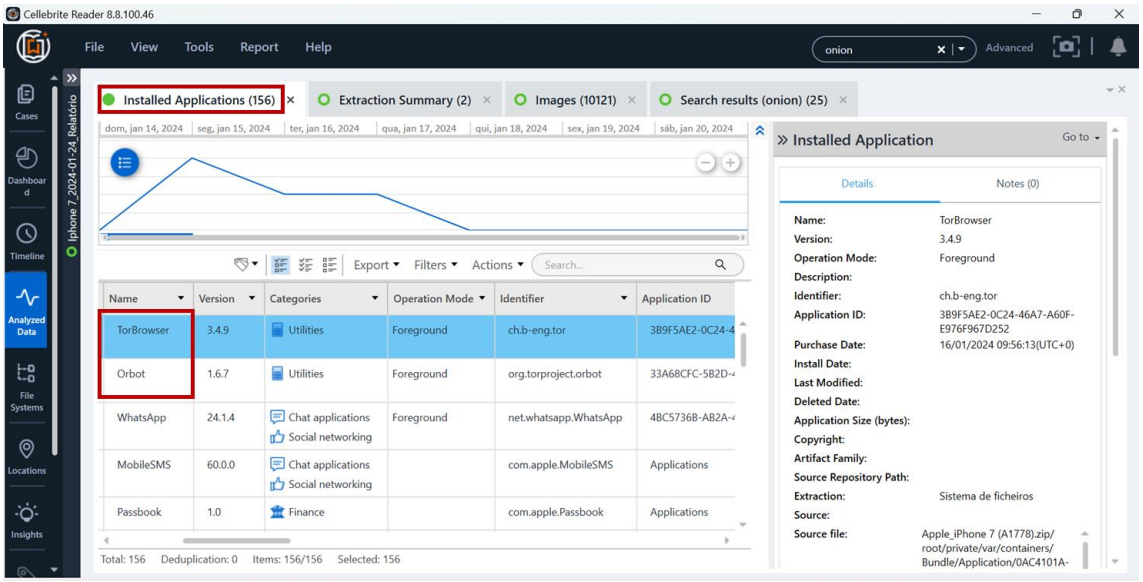
Figura 15. Dados obtidos através da extração lógica (Correio Eletrónico)



Outrora, para efeitos da investigação, não basta apenas localizar uma conta de correio eletrónico como é indispensável descobrir o seu titular. Para tal, analisa-se e interpreta-se o cabeçalho técnico das mensagens de correio eletrónico que contêm a informação do seu percurso e, em última instância, o IP associado. Posteriormente, solicita-se aos privados (*Internet Service Provider* (ISP) ou operadoras de telecomunicações) o seu titular.

Outro ponto a ter em conta é a instalação do browser *Tor*[48] e o aplicativo *Orbot* que, em conjunto, permitem ocultar a navegação, mantendo qualquer pesquisa sob o anonimato descrito no subcapítulo 2.4. E apesar de não ter sido possível a extração do histórico Tor, é possível argumentar sobre uma provável relação entre os links *onion* partilhados via correio eletrónico e a instalação deste browser, tendo em conta que só por este meio podem ser acedidos (Figura 16).

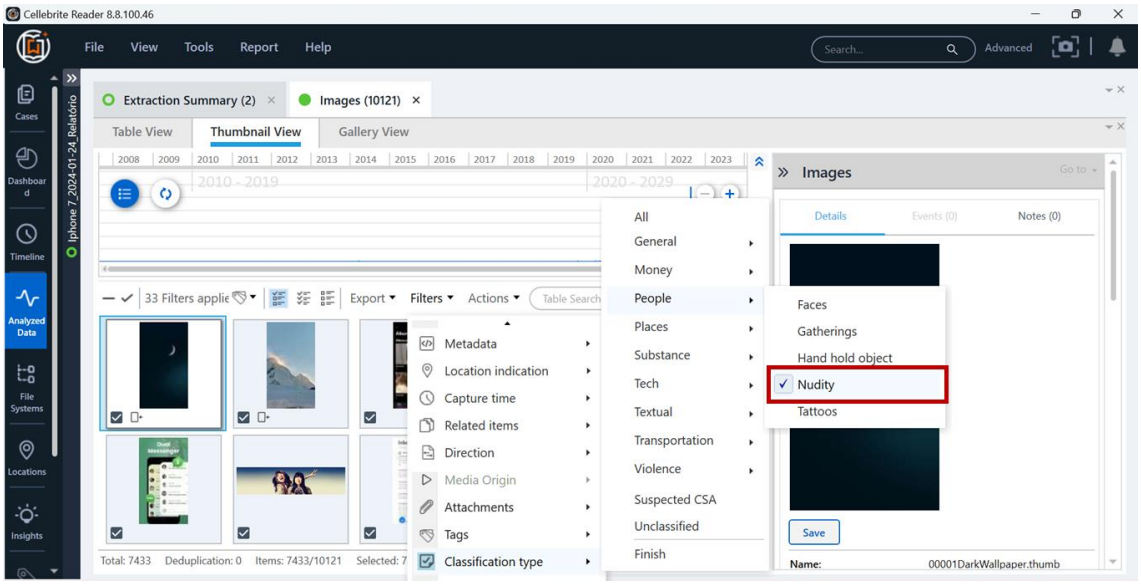
Figura 16. Dados obtidos através da extração lógica (Aplicações)



No decorrer desta perícia, foi igualmente encontrado material de ESM na galeria de fotos, através de uma filtragem de conteúdo: “Classification type” - “People” - “Nudity” (Figura 17). O programa, através de uma leitura inteligente e para cada fotografia, oferece uma percentagem que poderá representar nudez. Esta é uma das formas de detetar fotografias ou vídeos alusivos a ESM, no sistema informático.

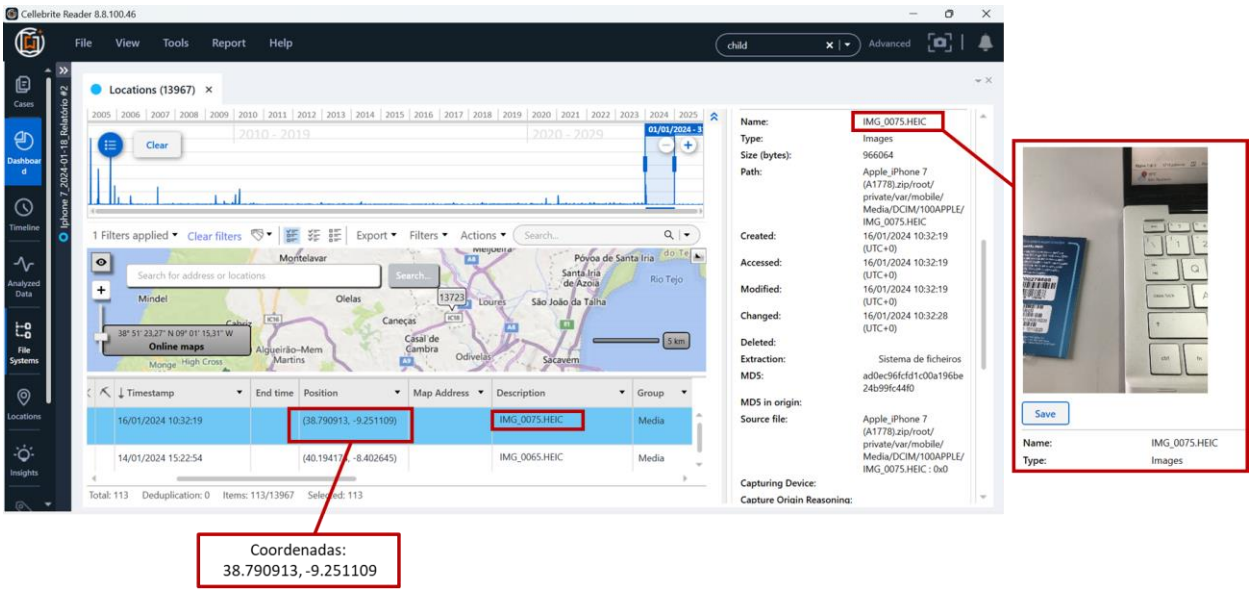
[48] Tor, um acrónimo para *The Onion Router,* é um motor de pesquisa desenhado para impedir a pegada digital, permitindo ao navegador uma pesquisa desprovida de qualquer tipo de filtragem sobre o seu conteúdo. A título de exemplo, o Chrome, devido à sua política de privacidade e segurança, impede a pesquisa e disseminação de conteúdo ilegal ou abusivo, contrariamente ao Tor que possibilita uma navegação e partilha de conteúdo totalmente livre. Esta é uma das razões para ser utilizado para atividades ilícita. Utiliza o sufixo .onion (semelhante ao conhecido .pt ou .com).

Figura 17. Dados obtidos através da extração lógica (Galeria de Fotografias)



Para além disso, fotografias e vídeos poderão conter dados de localização de onde foram realizadas, imensamente pertinentes para efeitos de uma investigação. Como observável na Figura 18, é possível verificar a data e hora em que foi produzida uma fotografia ou vídeo bem como as coordenadas por eles oferecida e os restantes metadados (no retângulo do lado direito).

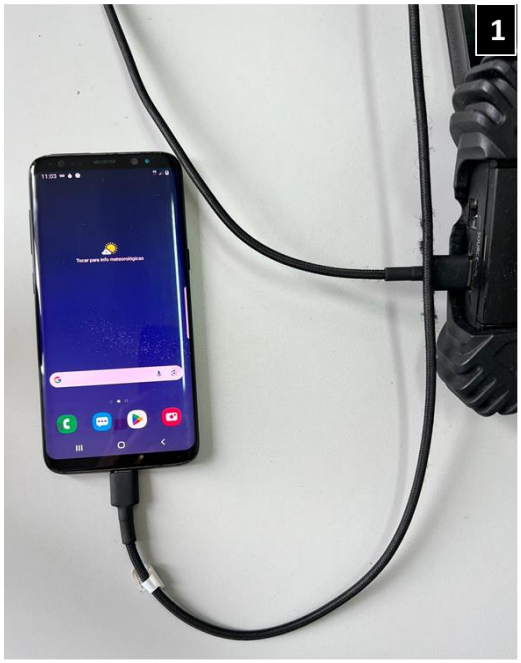
Figura 18. Dados obtidos através da extração lógica (Localização)



4.3.2 Samsung Galaxy S8

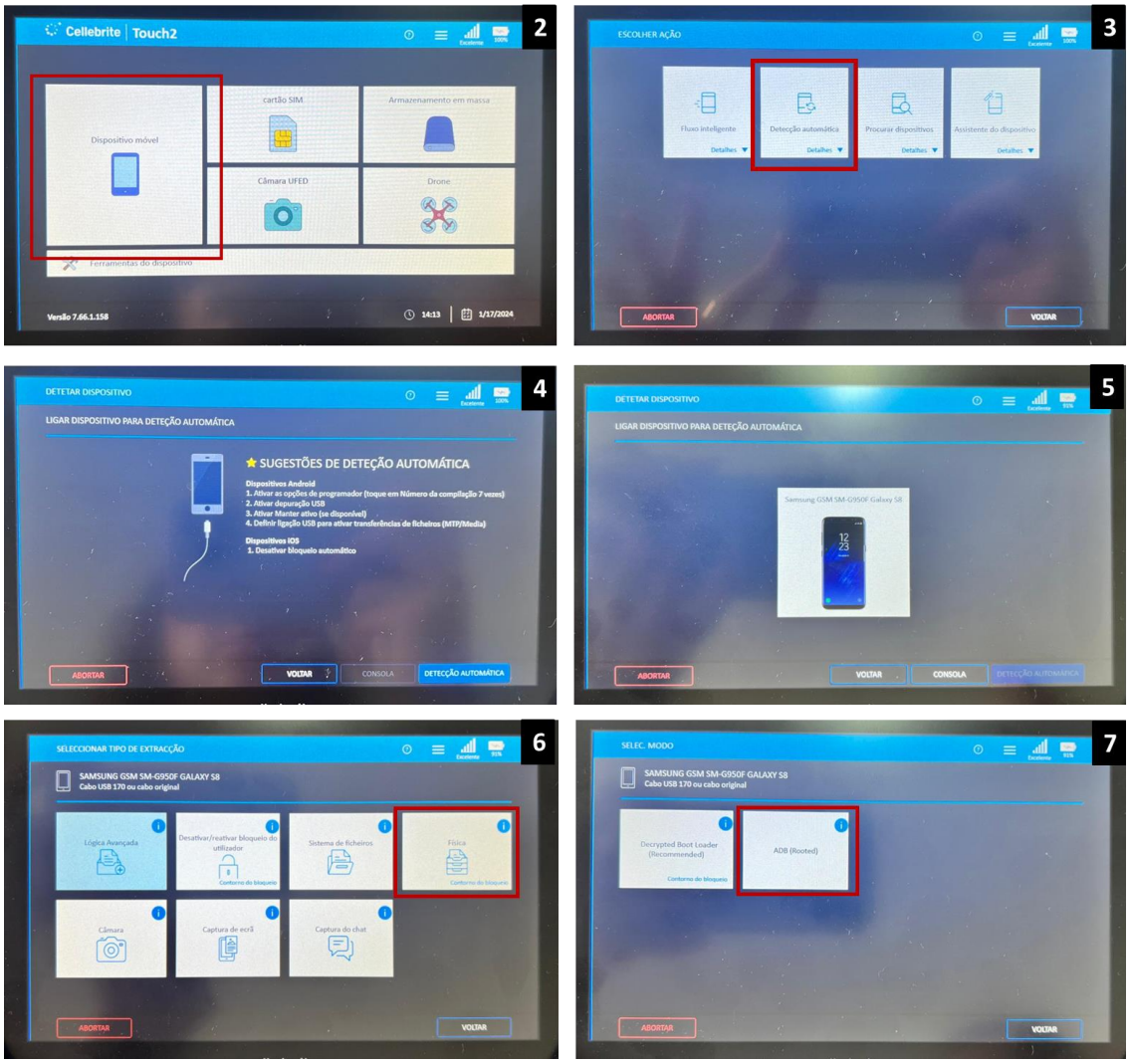
Analisados os dados do primeiro telemóvel (IPhone 7), procedamos à extração dos dados do Samsung Galaxy S8, ligando o dispositivo móvel ao equipamento *Cellebrite UFED Touch 2* através de um cabo USB.

Figura 19. Processo de Extração Física de dados do Samsung Galaxy S8 (Passo 1)



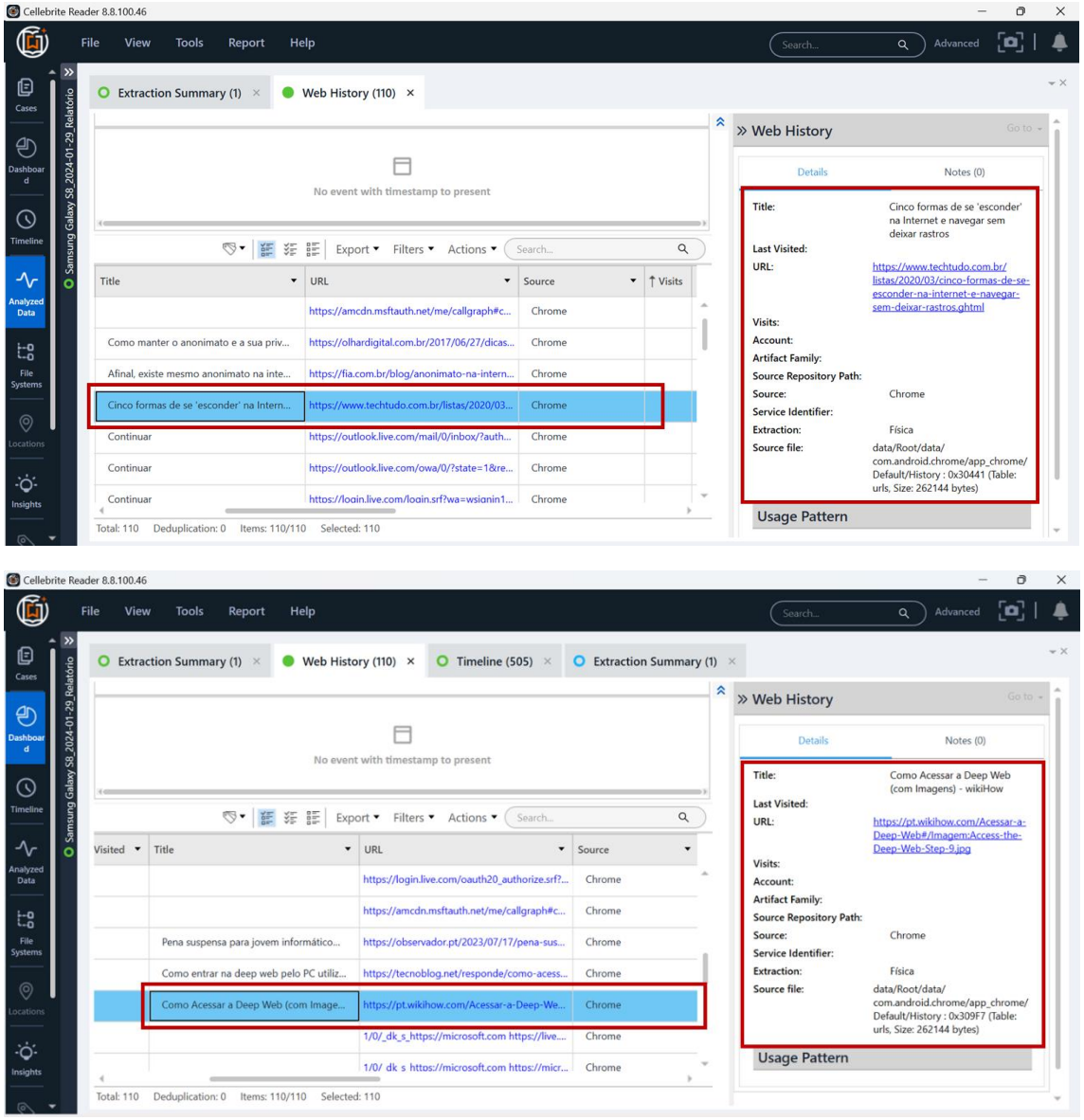
O mesmo processo se repete, porém, contrariamente ao IPhone 7, para o telemóvel Samsung é-nos possibilitada uma série de outras opções de extração (Passo 6), onde se enquadra a Extração Física, cuja principal diferença para o tipo de extração efetuada anteriormente (Lógica Avançada) reside na possibilidade de recolher itens eliminados, como SMS, registos de chamadas, entradas da lista telefónica, fotografias e vídeos. É a mais invasiva e abrangente de todas as extrações, incluindo todo o espaço não alocado no telemóvel, motivo pelo qual inclui dados eliminados. Neste caso, para extrair 64GB foram necessários 23 minutos.

Figura 20. Processo de Extração Física de dados do Samsung Galaxy S8



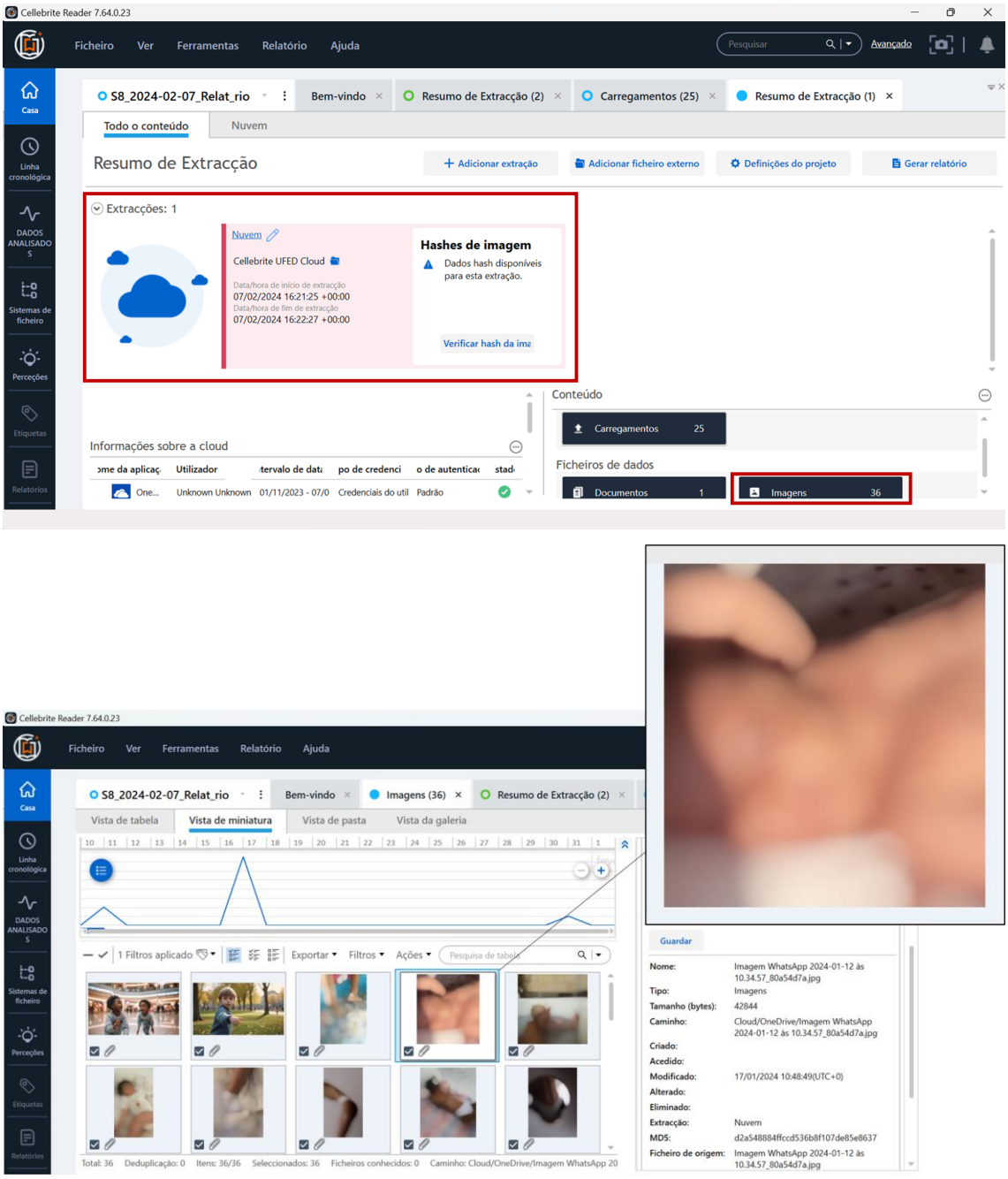
Realizada a extração, o passo seguinte será a análise da informação recolhida através do *software Cellebrite Physical Analyser* que fornece as mesmas opções que o caso acima retratado. Ora, deste telemóvel foi possível retirar igualmente informações sobre mensagens trocadas via SMS, correio eletrónico e para além do Whatsapp, via Telegram, que denunciam conteúdo de exploração sexual de menores. Tratando-se de uma situação idêntica em supra descrita, não é do nosso interesse ilustrar todos estes passos, todavia, o mesmo não acontece com os dados relativos ao histórico de pesquisa (Figura 21) e à nuvem (Figura 22).

Figura 21. Dados obtidos através da extração lógica (Histórico de pesquisa)



Ora, foi possível apurar que foram realizadas pesquisas no browser Chrome que conduziram ao acesso a sites “Cinco formas de se esconder na Internet e navegar sem deixar rastros” ou “Como Acessar a Deep Web (com imagens) - wikiHow” que poderão levantar suspeitas quanto à sua intenção.

Figura 22. Dados obtidos através da extração lógica (Nuvem)

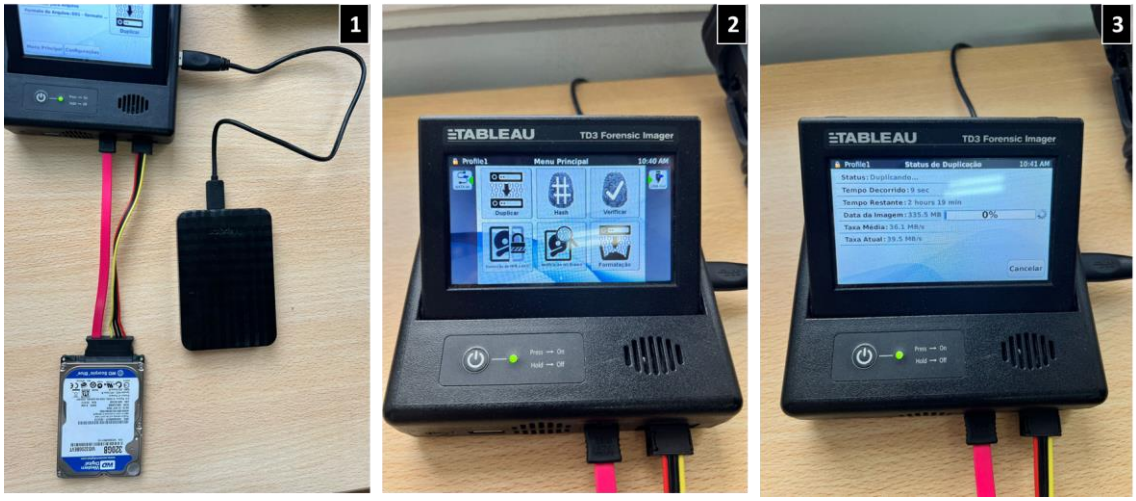


Posteriormente, realizou-se a extração dos dados da Nuvem, uma opção possibilitada pelo *software Cellebrite Reader*. A nuvem permite armazenar informação num espaço virtual, todavia, apesar da panóplia de vantagens por ela oferecidas, representa uma das maiores dificuldades das forças de segurança do digital forense na recolha de Prova Digital, face à facilidade de adulterar ou eliminar qualquer tipo de dados com recurso a outro sistema informático. Neste caso, acedidas as imagens contidas na nuvem, foi encontrado conteúdo de ESM, como visível na Figura 22.

4.3.3 Toshiba NB305-10GB

Como referido no corpo do trabalho de investigação, os diferentes sistemas informáticos exigem, por vezes, diferentes *softwares* de extração e análise. Para aquisição dos dados do computador Toshiba NB305-10GB, foi-lhe retirado o disco de memória, posteriormente ligado ao equipamento *Tableau TD3* através de um cabo SATA. No mesmo equipamento foi ligado um disco externo através de um cabo USB que receberá a totalidade dos dados extraídos, efetuando-se, assim, uma cópia (Figura 23).

Figura 23. Processo de Extração Física de dados do Toshiba NB305-10GB

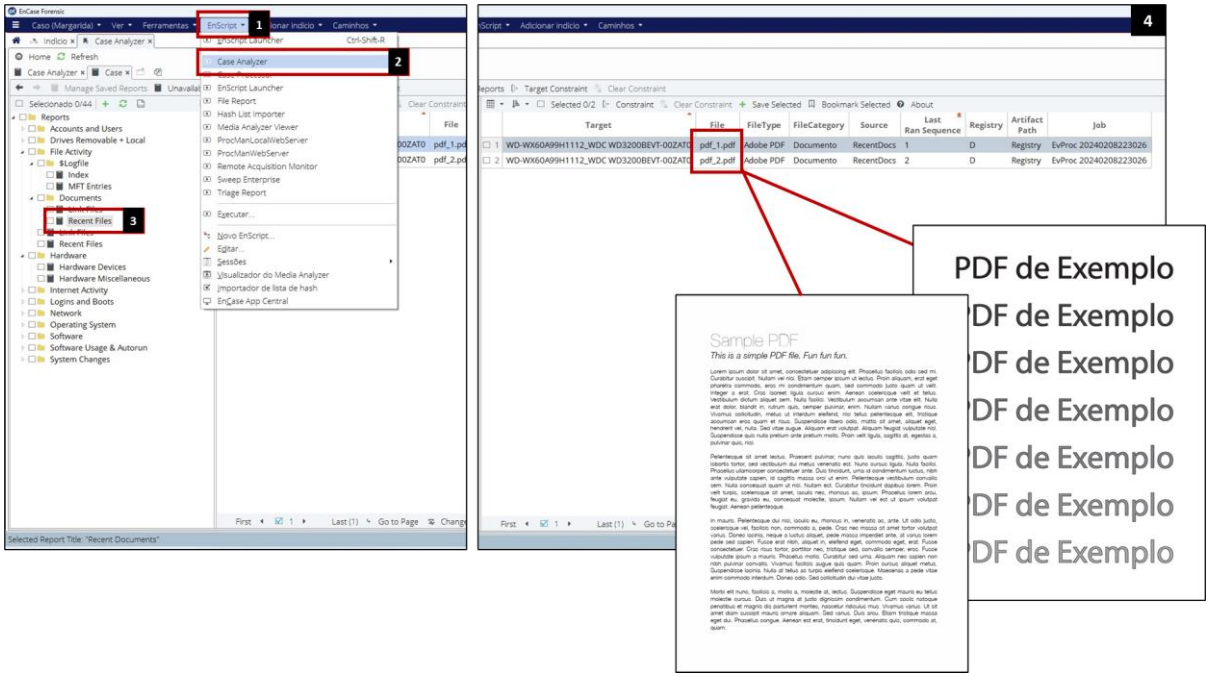


Ora, a extração física forense de 16GB totalizou 2 horas e 19 minutos. O passo seguinte será a análise da informação recolhida através do *software OpenText EnCase Forensic.* E contrariamente ao *Cellebrite Physical Analyser*, mais intuitivo e visual, o *software OpenText EnCase* necessita de um conhecimento mais aprofundado para seu manuseamento e, como tal, apenas serão indicados os passos a seguir nas situações específicas que pretendemos demonstrar. Feita esta ressalva, é possível argumentar sobre um conjunto de dados que denotam ESM.

Ora, uma forma extremamente comum de manter atividade criminosa sem a deteção por parte das autoridades é, de facto, a utilização de ficheiros para ocultar qualquer outro tipo de ficheiro (texto ou imagens, por exemplo), ou por outras palavras, troca de informação

escondida. Todavia, é possível detetá-los no Digital Forense[49] e, neste caso, foram encontrados dois pdfs "pdf_1" e "pdf_2" (Figura 24), sobre as quais recaem suspeitas de conterem material de ESM. Esta é a particularidade deste método na ocultação de conteúdo (muitas vezes ilegal) tendo em conta que, aparentemente, não se levanta qualquer tipo de desconfiança quanto ao seu conteúdo e, por isso, considerado bastante eficaz.

Figura 24. Análise de dados do Toshiba NB305-10GB



Por forma a localizarem-se possíveis ficheiros ocultos, primeiramente, é necessário instalar um *software* de visualização de ficheiros em modo hexadecimal (no caso, o HxD, um editor hexadecimal gratuito, adequado para o sistema operacional Microsoft Windows) que deverá ser aberto e nele descarregado o PDF que se pretende analisar, neste caso o "pdf_2".

Ora, como observável na Figura 25, a primeira etapa passa por "Localizar" e, posteriormente, procurar na barra de pesquisa a sigla "eof"[50] que designa *End Of File,* ou em português, Fim do Ficheiro, onde o código PDF deverá terminar. Deste modo, poderemos obter confirmação sobre a existência de outro ficheiro contido no PDF que, caso exista, encontrar-se-á codificado logo após a sigla "eof".

[49] Ressalva-se que, apesar de possível, não existe qualquer evidência que permita concluir que um ficheiro contém informação oculta. Para tal, é necessário que recaiam fundadas suspeitas sobre a existência de material ílicito nestes ficheiros para, posteriormente, serem periciados e investigados.

[50] Esta sigla é exclusiva dos ficheiros PDF. No caso de ficheiros JPEG, por exemplo, a sigla que indica o fim da imagem será diferente. Consultar https://docs.fileformat.com/pt/image/jpeg/ para obter referências sobre a designação hexadecimal por tipologia de documento.

Figura 25. Processo de localização de um ficheiro oculto num PDF (Passo 1 e 2)

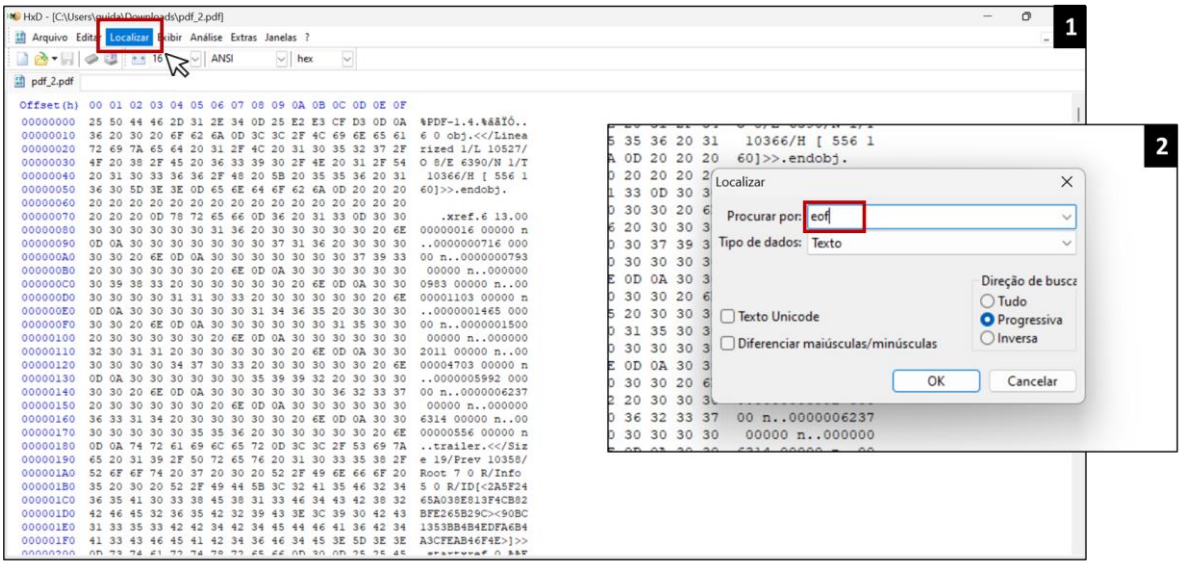
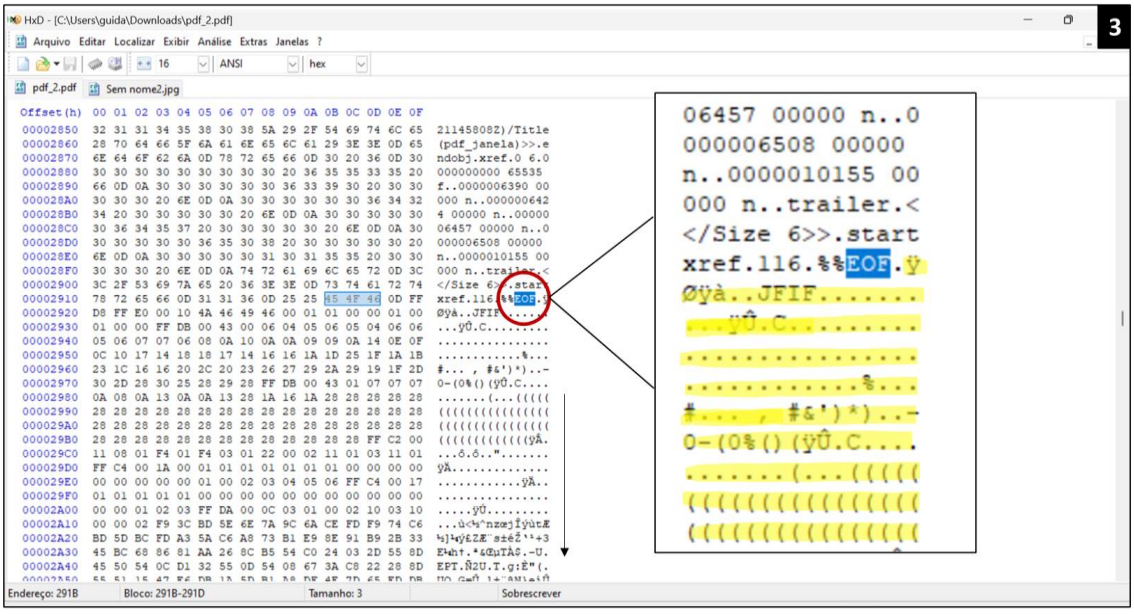
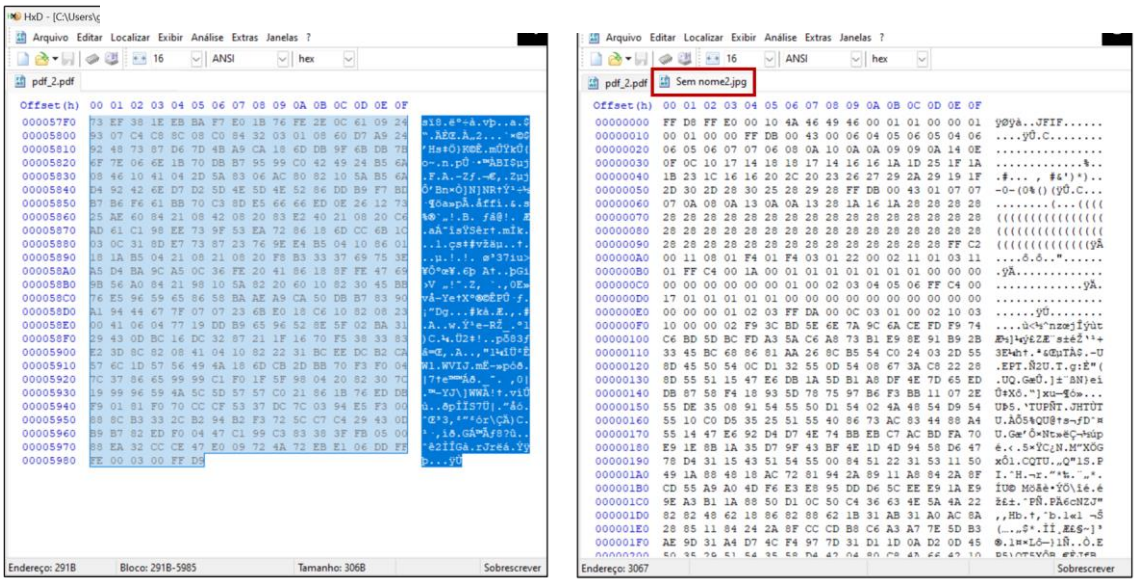


Figura 26. Processo de localização de um ficheiro oculto num PDF (Passo 3)



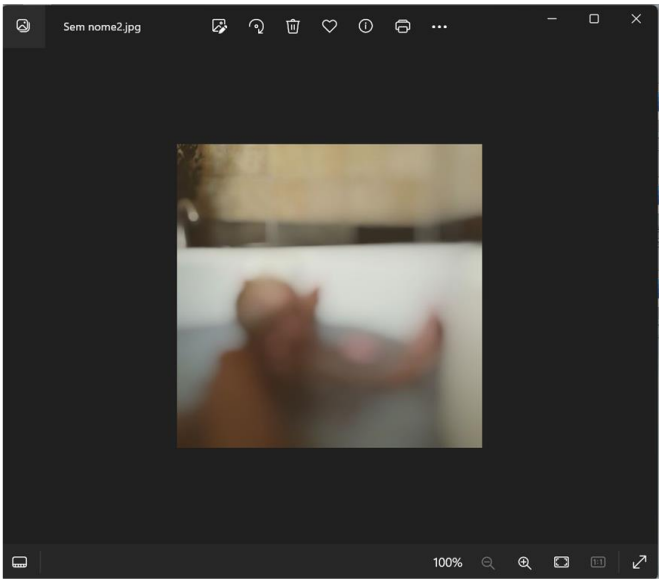
Como visível na Figura 26, é possível constatar a existência de outro ficheiro (sublinhado a amarelo) contido no PDF, neste caso, uma imagem (designação de JFIF). Posteriormente, será necessário copiar este código (desde o "ÿ" inicial até ao último caractere) como visível no passo 4 da Figura 27 e, de seguida, abrir nova página e colá-lo na íntegra (passo 5).

Figura 27. Processo de localização de um ficheiro oculto num PDF (Passo 4 e 5)



O ficheiro "Sem nome 2. jpg" deverá ser guardado e, quando acedido, terá o aspeto retratado na Figura 28.

Figura 28. Ficheiro JPG

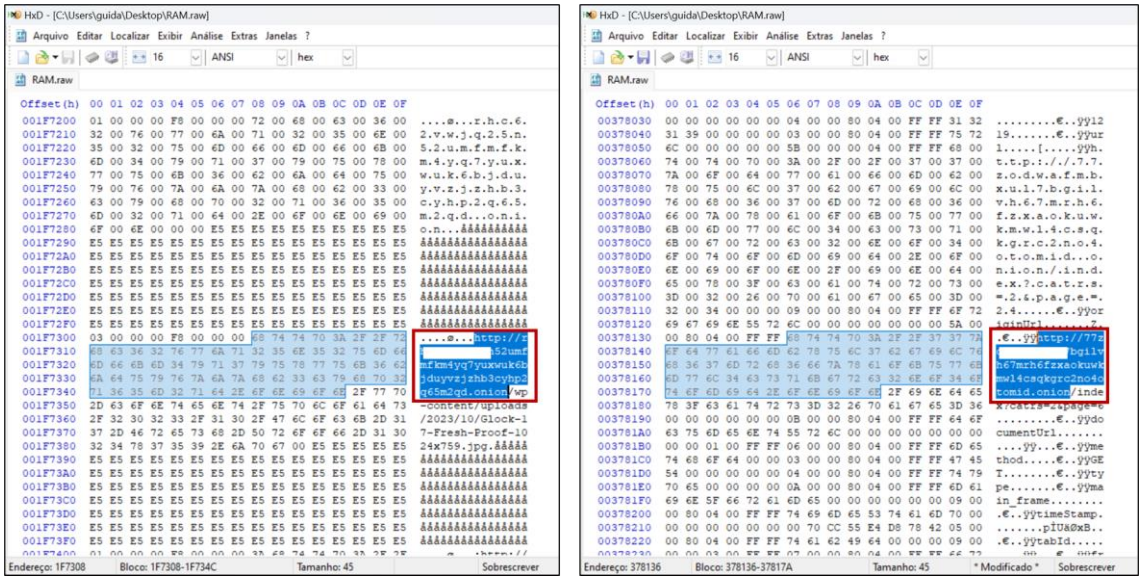


De seguida, é fulcral focarmos a nossa atenção no histórico de pesquisa. Através deste método de extração apenas é possível aceder ao histórico de pesquisa nos browsers instalados no computador - caso do Chrome e Mozilla Firefox - não tendo sido encontrada nenhuma evidência sobre a prática deste crime e, visto que o acesso a conteúdo de ESM é bastante comum na darknet, é necessária uma vez mais procurar indícios desta atividade por meio do TOR browser. Para tal, e figurando um outro cenário de obtenção de dados (*live forensics)*,

realizou-se uma extração da memória RAM[51] do computador, enquanto o mesmo se encontrava ligado pois só assim poderemos assegurar que o TOR não elimina o conteúdo do histórico de pesquisa.

Após a extração, o ficheiro obtido da memória RAM foi aberto através do *software* HxD, e o passo seguinte passou por localizar a sigla *onion* com o objetivo de identificar os sites acedidos na *dark web*. Como visível na Figura 29, foram encontrados sites que, quando verificados, confirmaram sites de pornografia infantil.

Figura 29. Histórico de pesquisa do TOR browser



4.4. Apresentação e Discussão de resultados

Durante a realização do estágio curricular, que decorreu nas instalações do Departamento de Investigação Criminal da Direção Nacional da PSP ao longo de um período de 6 meses, foi possível adquirir um leque abrangente de conhecimentos relativos, nomeadamente, à aquisição e análise de dados de sistemas informáticos, bem como as dificuldades encontradas na sua execução, as ferramentas e métodos forenses utilizados para a valoração da prova digital e o funcionamento e estrutura da investigação criminal da PSP.

[51] Nem sempre é possível fazer este tipo de extração visto que, por muitas vezes, o primeiro contacto dos *first responders* com os sistemas informáticos acontece quando os mesmos se encontram desligados.

Após o caso prático desenvolvido, resta-nos discutir resultados e comparar os sistemas informáticos, nomeadamente no que diz respeito aos dados que foram possíveis de extrair de cada um. Para tal, foram feitas 3 tabelas para que a comparação se torne mais intuitiva e visual.

A mais notável diferença entre os dois telemóveis (IPhone 7 e Samsung S8) diz respeito ao tipo de extração permitida. O IPhone possui particularidades no seu sistema operativo (iOS) que impede os *softwares* forenses em uso da PSP de realizar uma extração física, sendo apenas possível a extração lógica avançada, isto é, uma extração menos aprofundada. Esta é uma das causas que justifica a diferença entre os dados obtidos do IPhone face ao Samsung, *e.g* das fotografias eliminadas, os sites acedidos e ainda o acesso à nuvem, dados possíveis de consultar no caso do Samsung 8 (Tabela 7) mas não no IPhone 7.

Outrora, ainda no caso do Samsung 8, apesar de recuperadas fotografias apagadas, o *software* somente permitiu a visualização de uma parte (em 5 só foi possível recuperar 2). Apenas se tem conhecimento desta situação pois os conteúdos eliminados foram registados na tentativa de fazer uma análise o mais rigorosa quanto possível. Esta pode ser identificada como uma limitação do *software Cellebrite Physical Analyser* neste caso em concreto - pois depende do dispositivo móvel em causa - visto que é importante a recuperação e visualização total do conteúdo eliminado na eventualidade de conter material ilegal.

Tabela 6. Análise dos dados extraídos do IPhone 7

Extração Lógica Avançada	O que foi efetuado?	O que foi encontrado?
Galeria de Fotografias	Fotografias capturadas	✓
	Fotografias eliminadas	✗
Mensagens	Mensagens via SMS	✓
GPS	Dados de localização	✓
Correio Eletrónico	Ficheiros enviados	✓
	Contas de e-mail	✓
Redes Sociais	Mensagens via Whatsapp	✓
Aplicações	Aplicações descarregadas	✓
Histórico de Pesquisa	Sites acedidos Safari	✗
	Pesquisas realizadas Safari	✗
	Sites acedidos TOR	✗
	Pesquisas realizadas TOR	✗
Nuvem	Ficheiros vídeo e/ou imagens	✗

Legenda:
✓ Foi encontrado dentro de algumas especificidades; ✓ Foi encontrado. ✗ Não foi encontrado.

Tabela 7. Análise dos dados extraídos do Samsung S8

Extração Física	O que foi efetuado?	O que foi encontrado?
Galeria de Fotografias	Fotografias capturadas	✓
	Fotografias eliminadas	✓
Mensagens	Mensagens via SMS	✓
GPS	Dados de localização	✓
Correio Eletrónico	Ficheiros enviados	✓
	Contas de e-mail	✓
Redes Sociais	Mensagens via Whatsapp	✓
Aplicações	Aplicações descarregadas	✓
Histórico de Pesquisa	Sites acedidos Chrome	✓
	Pesquisas realizadas Chrome	✓
	Sites acedidos TOR	✗
	Pesquisas realizadas TOR	✗
Nuvem	Ficheiros vídeo e/ou imagens	✓

Legenda:
✓ Foi encontrado dentro de algumas especificidades; ✓ Foi encontrado. ✗ Não foi encontrado.

Outro ponto que é possível concluir é a impossibilidade de obtenção de dados pesquisados no browser TOR, em ambos os sistemas informáticos. Seria de esperar que estes pudessem ser obtidos, no entanto, o mesmo não foi possível verificar. Este cenário reforça a retórica sobre impermeabilidade da atividade nele ocorrente (derivada da cifragem da navegação), condicionando o seu rastreamento por parte das autoridades. Esta é uma problemática não só presente nas FSS portuguesas como ao nível internacional.

Também no Toshiba confrontamo-nos com a mesma dificuldade, porém, ainda que por outra via (*live forensics*), foi possível aceder ao histórico do TOR (apenas aos sites acedidos e não às pesquisas concretas). No que concerne ao acesso dos dados guardados na nuvem, a mesma consegue ser acedida pelo *OpenText EnCase Forensics*, todavia, para tal, é necessário obter a respetiva palavra-passe.

Tabela 8. Análise dos dados extraídos do Toshiba NB305-10G

Extração Física	O que foi efetuado?	O que foi encontrado?
Ficheiros e Documentos	Documentos PDF	✓
GPS	Dados de localização	✓
Correio Eletrónico	Ficheiros enviados	✓
	Contas de e-mail	✓
Histórico de Pesquisa	Sites acedidos Chrome	✓
	Pesquisas realizadas Chrome	✓
	Sites acedidos TOR	✓
	Pesquisas realizadas TOR	✗
Nuvem	Ficheiros vídeo e/ou imagens	✓

Legenda:
✓ Foi encontrado dentro de algumas especificidades; ✓ Foi encontrado. ✗ Não foi encontrado.

Feita esta análise, é indispensável confrontar os princípios teóricos supramencionados com a realização da perícia digital forense. Efetivamente, conclui-se que a prática vai ao encontro aos princípios teóricos supramencionados, desde a realização de uma cópia forense para um suporte autónomo de armazenamento, à triagem da informação com recurso a quesitos de investigação.

No entanto, persiste um problema que reside no próprio suporte teórico. Como anteriormente mencionado, em Portugal não existe um manual único de procedimentos devidamente regulamentado e com sustentação teórica, comum a todas as FSS que atuem no domínio das perícias digitais, apenas recomendações de melhores práticas definidas internacionalmente. Os procedimentos nacionais a seguir são internamente definidos, podendo variar de acordo com instituição e que, no caso em particular da PSP, estão definidos no Manual Técnico de Preservação e Recolha da Prova digital na Investigação Criminal. Este Manual, de 2015, funciona como um suporte essencial de linhas orientadoras, porém, apenas num cenário de primeiro contacto com o local de busca juntamente com os métodos a seguir para uma devida preservação e manutenção da cadeia de custódia da prova, de forma generalizada. De facto, os nossos peritos informáticos forenses não possuem nenhuma base documentada e rigorosa de técnicas pelas quais se deverão reger em múltiplos cenários. Confrontar o trabalho mais operacional com a teoria conforme nos propusemos é, por este motivo, mais dificultado.

Para além disso, trata-se ainda de um Manual de 2015, sobre um tema que evolui a uma velocidade alarmante, sendo por isso sensato afirmar que será obsoleto em prol da realidade atual.

Acrescenta-se ainda que, em muitos momentos é-nos[52] vendida a ideia de uma polícia capacitada, capaz de responder a muitas das adversidades impostas pelo digital. Neste sentido, a teoria colide com a prática, pois pode concluir-se que um indivíduo munido dos conhecimentos técnicos necessários poderá contornar, com relativa eficácia, os métodos e ferramentas em posse das autoridades portuguesas e, assim, impossibilitar a constituição de prova digital. Para dificultar o trabalho dos peritos forenses, basta começar por fazer uso de um sistema informático mais moderno, com cifragens mais complexas[53].

Outrora, ainda assim, poderemos afirmar que todo o trabalho realizado pela Polícia de Segurança Pública, neste domínio, foi de encontro às expectativas no sentido em que, apesar de apresentar vulnerabilidades e se confrontar com falta de meios num 'vazio' normativo, movimenta-se de forma bastante habilidosa em matéria de investigação criminal e peritagem.

Para além do referido, ainda que não descrito no presente trabalho, será importante mencionar que foi utilizado um outro *software* (MSAB XRY) para comparação de resultados com o *Cellebrite Physical Analyser,* no caso do Samsung S8. Através dessa mesma análise apurámos que, em determinadas circunstâncias, ambos ofereciam diferentes informações e é, por isso, fulcral assegurar a utilização de diferentes *softwares* com o objetivo de complementar informação e, assim, contribuir para a condenação daqueles que se dedicam a práticas criminosas como o ESM.

Estes factos permitem-nos concluir que o tipo de investigação aqui realizado é essencial para testar a eficácia de alguns procedimentos, técnicas e materiais em uso das polícias portuguesas, e com isso identificar vulnerabilidades e apresentar respostas para uma melhor resposta futura. Em específico, reproduzir o trabalho realizado no Setor Digital Forense do Laboratório de Criminalística e Ciência Forense serve igualmente para aproximar a comunidade académica da praticidade do cenário policial em casos que ocorram neste mundo que se impõe (o Ciberespaço).

[52] Civis.

[53] Por uma questão de segurança, não serão dados pormenores mais técnicos e outros exemplos que provem este argumento.

Conclusões e considerações finais

A bibliografia sobre Ciberespaço é bastante abrangente nas suas mais variadas vertentes, bem como a bibliografia referente à exploração sexual de crianças e ainda à prova digital, sendo este um dos motivos que nos permitiu arquitetar esta dissertação numa base sólida. O estágio curricular permitiu a aprendizagem através do método da observação e da aplicação dos conhecimentos adquiridos, conferindo ao trabalho o corpo necessário para apresentar conclusões devidamente sustentadas.

Todo o trabalho de pesquisa realizado até aqui, de cariz prático e teórico, acompanhado da experiência adquirida, culminaram na formação de uma opinião crítica sobre o assunto e permitiram solidificar a presente investigação. Como tal, foram encontradas respostas para todas as perguntas colocadas inicialmente e de modo a organizar o raciocínio, as mesmas foram individualmente respondidas.

Como evoluiu o regime jurídico da prova digital, na última década? Até 2012, data do estudo de Magriço, embora parte delas extremamente recentes, era possível debater sobre um conjunto de normas já existentes que regulavam a prova digital, descritas no subcapítulo 3.1.2.

Desde então, é crucial reconhecer algumas alterações introduzidas como resposta à evolução das TIC no âmbito da investigação criminal, nomeadamente o Regulamento (UE) n.º 910/2014 de 23 de julho, a Lei n.º 67/98 de 26 de outubro, alterada pela Lei n.º 58/2019, de 08 de Agosto (4ªa versão), a Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 16/2022, de 16 de agosto (3ª versão), a Lei n.º 109/2009 de 15 de setembro, alterada pela Lei n.º 79/2021, de 24 de novembro (2ª versão). Entre todas elas, destaca-se a Lei dos Metadados (Lei n.º 32/2008, de 17 de julho) face à nova realidade que instituiu.

Conclui-se que a última década foi marcada pela introdução de mudanças no regime jurídico referente à prova digital, outrora, considerá-las positivas é debatível, quer no meio político como académico. O quadro jurídico-legal português carece, ainda assim, de devida regulamentação nesta matéria, começando pela falta de uma definição legal de "Prova Digital" e "Cadeia de custódia da prova", necessárias para o devido enquadramento da prova não só do crime ocorrente no Ciberespaço, como do crime tradicional (no caso deste último). Adotando uma opinião crítica, seria de esperar que no espaço de 10 anos não nos confrontássemos, ainda, com um vazio jurídico neste domínio.

A nível nacional são seguidos procedimentos e metodologias de investigação padrão, neste âmbito? Ao longo de vários anos de experiência profissional, foi constatado por Marques (2013) que se verificavam inúmeros arquivamentos de processos face à falta de preservação de indícios ou prova digital, tendo em conta que a preparação dos intervenientes responsáveis em todo o processo (operacionais de sistemas informáticos, polícias, juristas) apresenta insuficiências. E apesar de se tratar de um testemunho não muito recente, consta-se que a preparação de todos os envolvidos que lidam com prova digital tem impacto direto na preservação da prova.

É facto que nos últimos anos a formação e qualificação destes profissionais tem sido evidenciada em relatórios institucionais como peça fundamental na IC, verificando-se um investimento neste sentido. Porém, garantir uma formação adequada não será concretizável sem recurso a uma devida regulamentação sobre o que deverá ou não constar, objetivamente, do trabalho destes intervenientes. Apesar de, em Portugal, serem adotadas recomendações internacionais de boas práticas nesta matéria (*e.g*. ISO 27037 de 2012, como explorado no capítulo 3.3.1), cada OPC trabalha de acordo com os procedimentos internos estabelecidos. Reconhece-se a necessidade de regulamentar e uniformizar algumas práticas gerais entre todos os OPC, nomeadamente os procedimentos de recolha de prova digital com vista a uma adequada preservação da prova, quebrando o ciclo que atualmente existe.

Na dimensão do Ciberespaço, quais as restrições às investigações nos casos de exploração sexual de menores? Através da técnica de observação e após a análise realizada no presente trabalho, poderá concluir-se que muito embora o Ciberespaço represente uma vantagem imensa para a investigação criminal, fornece um maior leque de soluções ao crime do que às autoridades policiais.

As investigações nos casos de ESM no Ciberespaço são, deste modo, extremamente dificultadas face ao anonimato proporcionado aos autores do crime (através da *darknet* e aplicações encriptadas), à ausência de um espaço físico onde é armazenada a informação (serviços *nuvem*) e onde o crime acontece, que permita facilmente definir o regime jurídico a aplicar. Acresce que a eficácia das investigações depende, em muitos momentos, da cedência de informação por parte dos privados (ISP) para obtenção de dados que permitam constituir prova, o que poderá representar um entrave, como vimos no capítulo 3.1.2.

Estará a lei portuguesa em conformidade com as necessidades exigidas por este tipo de atividade criminal? Este é um problema de dimensão global, porém, a lei portuguesa deverá, claro, adaptar-se à realidade nacional e para tal é necessário analisar as ocorrências criminais

em Portugal alusivas à ESM *online*. Os dados fornecidos pelas Estatísticas da Justiça revelam que as autoridades policiais registaram um total de 964 crimes de abuso sexual de menores em 2022, superando os 828 assinalados em 2021 e os 843 contabilizados em 2020. Ainda assim, a porta-voz da UNICEF Portugal Beatriz Imperatori[54], aponta que os números estão aquém da realidade se os cálculos tiverem por base os valores de referência da Organização Mundial de Saúde (OMS), que regista cerca de 140 mil crianças possivelmente vítimas deste tipo de abuso, em Portugal ao ano de 2022. Desde a sua criação em 2015, a base de dados de condenados por crimes sexuais em Portugal registou no total cerca de 7 387 ocorrências criminais de abuso sexual de crianças, dizem ainda os dados do Ministério da Justiça.

Porém, atualmente, não existe diferenciação na apresentação de dados estatísticos quanto ao abuso sexual de menores cometidos através de recursos disponíveis no Ciberespaço, tal como Magriço refere em 2012. Este facto dificulta a análise da eficácia do quadro jurídico-legal português na resposta ao ESM que ocorre *online*, que deverá ser o mais autêntico possível para verdadeira perceção do problema e posterior adoção das medidas necessárias de combate e repressão do fenómeno.

Acrescenta-se ainda o acesso à justiça nos casos de ESM, em Portugal, considerado um "mau exemplo" por duas organizações internacionais defensoras dos direitos das crianças e jovens (*Brave Movement* e *Child Global*), quando comparado ao contexto europeu. Contrariamente a países como Reino Unido, Irlanda e Bélgica - classificados como os que mais protegem as menores vítimas desta forma de crime - Portugal pertence ao grupo de países que pior se posiciona no que respeita à prescrição de crimes de abuso sexual, que começa a contar a partir do dia em que o crime é cometido. Este é, de igual modo, um problema que pode ser arrastado para a vertente *online*.

Estes são alguns exemplos que nos permitem concluir que o nosso quadro legal relativo a esta matéria poderá necessitar de algumas adaptações.

Deveremos dotar os nossos OPC de competência genérica de maiores competências de IC, nesta matéria? No que respeita às competências da Polícia de Segurança Pública para fins de investigação criminal é possível constatar que, como referido no art. 3º, nº2, alínea e) da Lei n.º 53/2007, de 31 de agosto (Lei Orgânica da PSP), lhe compete "Desenvolver as acções de investigação criminal e contraordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas". E como anteriormente

[54] Discurso resultante do grupo de trabalho para a avaliação da legislação sobre abusos sexuais de menores, na Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, a setembro de 2023.

referido, é a LOIC, no seu art. 6º, a responsável por delimitar os crimes da competência da PSP, órgão de polícia criminal de competência genérica (art. 3º. nº1, alínea c)). Da sua leitura apreende-se que à PSP (e à GNR) compete os crimes não reservados a outra polícia, mas também os crimes que dada a sua simplicidade, embora reservados, lhe possam ser atribuídos pela autoridade judiciária competente.

De facto, o que se pretende com isto é a atribuição dos crimes mais complexos e graves à PJ, dotada de competência especializada e munida de recursos, meios e técnicas que a compõem enquanto OPC por excelência, e que as demais investigações (simples e menos gravosas) pudessem ser atribuídas aos restantes OPC, onde se enquadra a PSP. Outrora, analisados estes artigos, parece-nos uma constatação relativamente vaga, sem a especificação dos tipos de crime da sua competência (PSP). Este facto é passível de gerar conflito de competências (cujo maior número se verifica justamente entre a PSP e a PJ) que Abreu (2012) define como "pântano legislativo".

Acresce que, desde a criação da LOIC em 2008, os OPC de competência genérica têm sido dotados de formação e meios alusivos à investigação criminal que lhes confere capacidade de investigar um conjunto de crimes definidos como exclusivos da PJ (onde são enquadrados os crimes "informáticos e praticados com recurso a tecnologia informática" (art. 7º, nº 3, alínea l)). Esta premissa é comprovada pelo MP que, ao longo dos anos, tem delegado à PSP crimes desta lista, fomentando-se uma relação de confiança com a instituição. Tomamos como exemplo recente o Caso Influencer, assistido em primeira mão pela Polícia de Segurança Pública na recolha de prova digital.

Relativamente à atividade criminal objeto de estudo do presente trabalho, diz-nos o RASI (2022) que, no caso português, as situações de abuso sexual *online* são normalmente praticadas por indivíduos isolados e em geral de nacionalidade portuguesa, ou residentes em PT, não assumindo, portanto, carácter de crime organizado internacional. Tratam-se, assim, de casos de menor complexidade que, no entanto, permanecem sob alçada da PJ. Como tal, não temos como não interrogar: tendo em conta o expressivo aumento da ESM *online*, porque não são delegadas competências de IC para OPC como a PSP, relativas a crimes de menor complexidade, de modo a libertar a Polícia Judiciária do dilúvio de crimes pelas quais são responsáveis e, assim, contribuir para a celeridade de algumas investigações?

E apesar da LOIC primar pelo seu carácter meramente orientador e não obrigatório – sendo, de facto, o MP o responsável por "Dirigir a investigação e as ações de prevenção criminal" (art.4, nº1, alínea e)) - questiona-se, ainda assim, a necessidade de reformulação de uma LOIC

obsoleta, para uma melhor definição dos crimes a investigar pelos OPC de competência genérica e, eventualmente, dotá-los de maiores competências de IC (nomeadamente da atividade criminal de ESM *online*).

Respondidas todas as perguntas derivadas, resta-nos dar resposta à pergunta cerne da investigação: "**Tendo em consideração a transferência para o Ciberespaço de atividade delituosa relativa à ESM é possível implementar procedimentos de investigação criminal que, com eficácia, acautelem a aquisição de prova digital e potenciem a condenação daqueles que se dedicam a tais práticas criminosas?"**

Face a um regime jurídico da prova digital, aquém do expectável face às necessidades impostas pelo crime no digital; a procedimentos e metodologias de investigação que necessitam de padronização nacional; a restrições acentuadas às investigações nos casos de ESM no Ciberespaço; a um quadro legal em matéria de ESM que poderá necessitar de adaptações; à falta de competências atribuídas legalmente a OPC externos à PJ; e ainda às conclusões retiradas da simulação da investigação, poderá concluir-se que a aquisição de prova digital para condenação daqueles que se dedicam a este tipo de crime, apesar de verificar progressos, necessita de aperfeiçoamento nos domínios mencionados para que seja cumprido o rigor exigido e assim ser verdadeiramente eficaz, nesta que é uma "[...] sociedade de risco associada a uma cultura do medo e da insegurança" (Beck, 1992, p. 19).

É fundamental vincar nesta conclusão que a atividade criminal de ESM trata-se de um crime contra crianças e jovens que coloca em causa a liberdade da autodeterminação sexual das mesmas. Como tal, o bem jurídico protegido é eminentemente pessoal e reside no livre desenvolvimento da personalidade do menor na esfera sexual (círculo mais íntimo da personalidade) (PJ, 2022). Acrescenta-se ainda que as práticas destas atividades são suscetíveis de provocar sintomatologia típica de desordem de stress pós-traumático (PTSD), possivelmente afetando o normal desenvolvimento dos jovens e crianças em diferentes contextos (*e.g.* contexto social, familiar, amoroso, e profissional, futuramente).

Todavia, no decorrer da investigação, fomos igualmente confrontados com dificuldades e limitações. Uma delas diz respeito à lacuna da bibliografia nacional quando conjugados os temas do Ciberespaço, ESM e prova digital num só, e ainda a inexistência e acesso a dados que permita quantificar o problema real da ESM (em situações em que se recorre a meios digitais), em Portugal. E tendo em conta que à Polícia de Segurança Pública não compete, legalmente, a peritagem e investigação de crimes de ESM, outra dificuldade encontrada respeita à dificuldade de aproximar a simulação elaborada a um caso anteriormente desenvolvido (pois dos arquivos

da PSP não constam este tipo de factos). A simulação baseou-se numa especulação do que seria caso a PSP tivesse espaço para intervir neste tipo de situações.

Retiradas todas as conclusões, é necessário sobre elas refletir. Será sensato afirmar que existem aspetos a aperfeiçoar que, aliados ao sentido crítico, nos permitem sugerir propostas de melhoria. Uma das primeiras recomendações diz respeito à necessidade de investimento contínuo em recursos materiais de modo a adequar o espaço de trabalho às funções a desempenhar - *e.g.* softwares forenses para a área do digital forense - que respondam às necessidades laborais e evolução tecnológica mundial para uma maior celeridade e eficácia nos processos. Este aspeto está intrinsecamente relacionado com as burocracias a nível interno nas instituições policiais portuguesas: a aquisição de equipamentos é, por exemplo, dificultada face ao demorado processo burocrático que a envolve.

Por outro lado, é fundamental apostar continuamente na qualificação e formação específica de recursos humanos alusivos à prova digital, representando este um ponto-chave para se fazer crescer na esfera da investigação criminal do digital. Toma-se como exemplo a cooperação com instituições, organizações e polícias estrangeiras, promovendo fóruns de discussão e formações em matéria de investigação criminal do digital, dando a conhecer outras formas e métodos de trabalho que poderão positivamente acrescentar valor a algumas práticas comumente utilizadas em Portugal (algumas delas já possivelmente obsoletas face à evolução do crime). Neste ponto acrescenta-se ainda uma continuada aposta em parcerias público-privadas que contribuirão para uma maior eficácia na realização de perícias e investigações que, no caso do digital, passa pelo fornecimento de dados pelas ISP e como supramencionado, a aquisição de equipamento e complementaridade na realização de perícias em casos específicos.

É igualmente imprescindível potenciar a contínua partilha e troca de informação entre órgãos de polícia criminal (GNR, PSP e PJ, por exemplo) que deverão basear-se em pressupostos de confiança e entreajuda; e ainda regulamentar algumas práticas (gerais) comuns a todos os OPC, nomeadamente os procedimentos de recolha de prova digital, alvo de análise da presente dissertação. O quadro jurídico-legal português necessita, assim, de uma reformulação nesta matéria, começando por apresentar uma definição legal de "Prova Digital" e "Cadeia de custódia da prova" para o devido enquadramento da prova não só do crime ocorrente no ciberespaço, como do crime tradicional.

Por fim, consciencializados sobre a evolução do crime com recurso a meios digitais, sendo a prova digital por vezes indispensável para condenar aqueles que cultivam este universo

que tira partido dos mais vulneráveis - crianças e jovens - a empatia para com estas situações nunca será suficiente. À equação deverá ser somada uma contínua problematização desta realidade, que não se delimita só à arena policial como pressupõe a complementaridade com outras áreas. Investigações numa ótica jurídica, da psicologia, sociologia, e do ponto de vista mais operacional (de computação) são essenciais para um estudo holístico do fenómeno para posterior apresentação de soluções dignas que protejam o direito de ser criança e jovem.

Bibliografia

Abreu, C. (2012). As Polícias, a Polícia Judiciária e o pântano legislativo. Modus Operandi, 5, 91-95.https://carlospintodeabreu.com/public/files/CPA_Policias_Policia_Judiciaria_pantano_legislativo.pdf

Akdeniz, Y. (2002). Anonymity, democracy and cyberspace. *Social Research, 69*(Nº1), 223-237. 10.1353/sor.2002.0010

Albuquerque, P. (2010). *Comentário do Código Penal à luz da CRP e da Convenção Europeia dos Direitos do Homem* (2ª ed.). Universidade Católica Editora.

Almeida, I. F. (2014). *A Prova Digital* [Dissertação de Mestrado]. Departamento de Direito da Universidade Autónoma de Lisboa. https://repositorio.ual.pt/bitstream/11144/1849/1/A%20prova%20Digital%20%28Dissertа%C3%A7%C3%A3o%29%20%281%29.pdf

Alves, F. & Pimentel, A., & Lapinha, C., & Gonçalves, J., & Guedelhas, S., & Marques, P., Veloso, L. (2015). Manual Técnico de Preservação e Recolha da Prova Digital na Investigação Criminal. Polícia de Segurança Pública.

Antunes, M., & Rodrigues, B. (2022). *Introdução à Cibersegurança: A internet, os aspetos legais e a análise digital Forense.* (2ª ed.). FCA - Editora de Informática.

Aras, V. (2015). *Crimes de informática - Uma nova criminalidade*. https://www.informatica-juridica.com/trabajos/crimes-de-informatica-uma-nova-criminalidade/

Barlow J. (1996). A Declaração de Independência do Ciberespaço. *Duke Law & Technology Review*, 5-7.

Basheer, R. & Alkhatib, B. (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. Hindawi Journal of Computer Networks and Communications, 2021. https://doi.org/10.1155/2021/130299

Bell, D. (1976). *The Coming of Post-Industrial Society. The Educational Forum, 40*(4), 574-579. *https://www.tandfonline.com/doi/abs/10.1080/00131727609336501*

Bell, D. (1979). *The Social Framework of the Information Society.* Michael L. and Moses, Joel (eds), 163–211.

Bell, D. (2001). *An introduction to cybercultures* (1ª ed.) London: Routledge https://dosengalau.com/wpcontent/uploads/2018/02/David_Bell_An_Introduction_to_Cyberculturesb-ok.org_.pdf

Borges, J. (2009). As novas e antigas ameaças para Portugal e Espanha: Perceções, Realidade e Prospectivas. *Revista Militar, Nº11*, 1425-1437.

https://comum.rcaap.pt/bitstream/10400.26/15123/1/Novas_Antigas_Amea%c3%a7as_Portugal_Espanha.pdf

Branco, J. R. (2021). *Prova Digital. Os meios de obtenção de prova digital e a restrição dos direitos do arguido* [Dissertação de Mestrado]. Faculdade de Direito da Universidade de Coimbra.https://estudogeral.sib.uc.pt/bitstream/10316/94718/1/Disserta%c3%a7%c3%a3o%20-%20Jos%c3%a9%20Ricardo%20Marques%20Branco%20-%20uc2012153587%20-%20pdf.pdf

Buzan, B. & Waever, O. & Wilde, J. de. (1998). *Security: A New Framework for Analysis.* (1ª ed). Boulder: Lynne Rienner.

Bygrave, L. & Bing, J. (2009). *Internet Governance: Infrastructure and Institutions* (1ª ed.). Oxford University Press.

Cancela, A. G. (2016). *A Prova Digital: Os meios de obtenção de prova na lei do cibercrime* [Dissertação de Mestrado]. Faculdade de Direito da Universidade de Coimbra. https://estudogeral.sib.uc.pt/bitstream/10316/31398/1/A%20prova%20digital.pdf

Castells, M. (1996). The Rise of the Network Society (2ªed). Blackwell Publishing Ltd https://deterritorialinvestigations.files.wordpress.com/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

Centro de Operações de Segurança Cibernética do Canadá (CSOC). (2018). Estratégia de Cibersegurança Nacional. A Visão do Canadá para a Segurança e Prosperidade na Era Digital. [PDF] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Centro Nacional de Cibersegurança (CNCS). (2019). Estratégia Nacional de Segurança do Ciberespaço 2019-2023. [PDF] https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

Centro Nacional de Cibersegurança (NCSC). (2022). Estratégia Nacional Cibernética: conduzir um futuro cibernético em todo o Reino Unido. [PDF] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

Clemente. P. (2015). *Cidadania polícia e segurança.* ISCPSI. http://id.bnportugal.gov.pt/bib/bibnacional/1917482

Código Penal, Decreto-Lei n.º 48/95. Diário da República n.º 63/1995, Série I-A de 1995-03-15.

Código Processual Penal, Decreto-Lei n.º 78/87. Diário da República n.º 40/1987, Série I de 1987-02-17.

Comissão Europeia (2014). *Electronic Evidence Guide – A basic guide for police officers, prosecutors and judges.* https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

Comissão Europeia. (2012). Estratégia europeia para uma Internet melhor para as crianças (COM(2012) 196 final) [PDF]. EUR-Lex. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012DC0196

Comissão Europeia. (2020). Estratégia da UE para uma luta mais eficaz contra o abuso sexual das crianças (COM(2020) 607 final) [PDF]. EUR-Lex. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0607

Conselho da Europa. (2005). Convenção do Conselho da Europa Relativa à Luta contra o Tráfico de Seres Humanos. https://rm.coe.int/168008371d

Conselho da Europa. (2017). Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais. Série de Tratados do Conselho da Europa, N.º 201. https://rm.coe.int/168046e1d8

Constituição da República Portuguesa. Diário da República n.º 86/1976, Série I de 1976-04-10.

Convenção sobre Cibercrime (2001), Resolução da Assembleia da República n.º 88/2009.

Cooper, W. (2009). The sexual exploitation of children and youth: redefining victimization. In Olfman, S. (Ed.), *The sexualization of childhood* (pp. 105–120). Westport, Estados Unidos da América: Praeger Publishers. ISBN 978–0–275–99985–8.

Costa, C. R. (2017). *As proibições de prova e a prova digital – aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade* [Dissertação de Mestrado]. Escola de Direito da Universidade do Minho. https://repositorium.sdum.uminho.pt/bitstream/1822/51857/1/Catarina%20Rodrigues%20Santos%20Costa.pdf

Creppell, I. (2011). The concept of normative threat. *International Theory V. 3*(Nº 3), 450–487. https://doi.org/10.1017/S1752971911000170

Dahlberg, L. (1998). Cyberspace and the Public Sphere Exploring the Democratic Potential of the Net. *Converge, V. 4*(Nº1), 71-84. https://doi.org/10.1177/135485659800400108

Daniel, K. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security*. National Defense University Press.

DataReportal. (2023). Digital 2023: France. Consultado a 29 de junho de 2023. https://datareportal.com/reports/digital-2023-france

DataReportal. (2023). Digital 2023: Germany. Consultado a 29 de junho de 2023. https://datareportal.com/reports/digital-2023-germany

DataReportal. (2023). Digital 2023: Italy. Consultado a 30 de junho de 2023. https://datareportal.com/reports/digital-2023-italy

DataReportal. (2023). Digital 2023: Portugal. Consultado a 30 de junho de 2023.https://datareportal.com/reports/digital-2023-portugal

DataReportal. (2023). Digital 2023: Spain. Consultado a 30 de junho de 2023. https://www.slideshare.net/DataReportal/digital-2023-spain-february-2023-v01

DataReportal. (2023). Digital 2023: Turkey. Consultado a 29 de junho de 2023. https://datareportal.com/reports/digital-2023-turkey

Davis, W. (2000). *Threats and promises: The pursuit of international influence.* MD: Johns Hopkins University Press.

Departamento de Defesa dos Estados Unidos. (2021). Dicionário Militar e Termos Associados. [PDF] https://irp.fas.org/doddir/dod/dictionary.pdf

Dijk, J. V. (2006). The Network Society (2ª ed.). Sage Publications Ltd. https://old.amu.ac.in/emp/studym/99998428.pdf

Du Pont, G. (2001). The criminalization of true anonymity in cyberspace. *Michigan Telecommunications and Technology Law Review, 7*(1), 192 - 215. https://repository.law.umich.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1142&context=mttlr

Eleutério, P. M., & Machado, M. P. (2014). *Desvendando a computação forense.* (1ª ed.). Novatec Editora Ltda.

Elias, L. (2011). *Segurança na Contemporaneidade: Internacionalização e Comunitarização.* Universidade Nova de Lisboa.

Elias. L. (2018). *Ciências Policias e Segurança Interna: Desafios e Prospetiva*. ISCPSI.

ENFSI. (2015). Best Practice Manual for the Forensic Examination of Digital Technology (vs. 01) https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

ENISA. (2019). ENISA Threat Landscape 2019.

ENISA. (2024). Glossário online da ENISA.

European Science Foundation. (2011). The European Code of Conduct for Research Integrity. Strasbourg: European Science Foundation.

Europol. (2023). *Internet Organised Crime Threat Assessment* 2023. Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

Europol. (2023). *Spotlight Report on Child Sexual Exploitation (2023).* https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-child-sexual-exploitation-iocta-2023

FBI. (2000). Digital Evidence: Standards and Principles. *Forensic Science Communications, 2*(2). https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

Fernandes, J. P. (2014). *Ciberguerra. Quando a Utopia se Transforma em Realidade* (1ª ed.). Verso da História.

Fernandes, M. (2018). *Da pornografia de menores em Portugal: Direito, políticas públicas e segurança*. Faculdade de Direito da Universidade Nova de Lisboa. [Dissertação de Mestrado] https://run.unl.pt/bitstream/10362/65277/1/CarrilhoFernandes_2019.pdf

Ferraro, M. & Casey, E. & McGrath, M. (2005). *Investigating Child exploitation and pornography: The Internet, the law and Forensic Science*. ISBN: 0-12-163105-2 Investigating Child exploitation and pornography: The Internet, the law and Forensic Science

Fidalgo, S. (2020). A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo. In Rodrigues, A. M. (coord.), *Inteligência artificial no Direito Penal*. Edições Almedina.

Freitas, J. P. (2017). *Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas* [Dissertação de Mestrado]. Escola de Direito da Univerisdade do Minho. https://repositorium.sdum.uminho.pt/bitstream/1822/64098/1/Disserta%c3%a7%c3%a3o%2bMestrado.pdf

Geraldes, S. M. (2019). A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista e/ou Otimista? *Nação e Defesa*, (N.º 154), 91-108. https://comum.rcaap.pt/bitstream/10400.26/33162/1/GERALDESSofiaMartins_Aestrat%c3%a9giadeciberseguran%c3%a7adaUni%c3%a3oEuropeia_Na%c3%a7%c3%a3oDefesa_N_154_p_91_108.pdf

Gibson, W. (1984). *Bur*ning *Chrome*. Harper Voyager

Gibson, W. (1984). *Neuromancer.* Asa

Giles, K. & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. In *5th International Conference on Cyber Conflict* (CYCON), Tallinn, Estonia. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6568390

Google. (2023). Privacidade e Termos de utilização. Consultado a 20 de junho de 2023. https://policies.google.com/privacy?hl=pt-PT#infosharing

Gouveia, J. (2023). *Os Novos Paradigmas do Direito Internacional Público.* [Comunicação oral]. II Congresso Luso-Brasileiro de Direito Internacional Público.

Granjo, P. (2006). Quando o conceito de «risco» se torna perigoso. *Análise Social, V. 41* (Nº 181), 1167-1179.

Guedes, A. M. (2006). O Pensamento Estratégico Nacional. Que futuro?. In José Nogueira, J. M. & Borges, J. V., *O Pensamento Estratégico Nacional.* (pp. 143-199).https://www.academia.edu/9273963/O_Pensamento_Estrat%C3%A9gico_Nacional_Que_Futuro

Guedes, M. (2015). Breves reflexões sobre Poder e Ciberespaço. *Revista de Direito e Segurança, 6,*189-209. https://comum.rcaap.pt/bitstream/10400.26/14329/1/PodereCiberesa%C3%A7o.pdf

Habermas, J. (1989). *The Structural Transformation of the Public Sphere* (5ª ed.). Polity Press.

Hauben, M. (1995). *The Net and netizens: the impact the Net has on people's lives.* https://catalogimages.wiley.com/images/db/pdf/0818677066.excerpt.pdf

Hermeiro, A. C. (2023). *A cadeia de custódia da prova digital: O uso da Tecnologia Blockchain como forma de preservação* [Dissertação de Mestrado]. Faculdade de Direito da Universidade de Coimbra. https://estudogeral.uc.pt/retrieve/259007/Dissertac%CC%A7a%CC%83o_AndreiaHermeiro.pdf

Honorato, M. C & Santos, L. F. & Mateus, R. M. (2017). *O ciberespaço como 5.º domínio operacional: impacto estratégico na política de Defesa Nacional* [Trabalho de Investigação]. Instituto Universitário Militar. https://comum.rcaap.pt/bitstream/10400.26/21956/1/07_TIG%20AEE%20-%20Ciberespa%c3%a7o%205%c2%ba%20Dominio%20de%20Opera%c3%a7%c3%b5es.pdf

INCIBE, APAV, Guarda Civil Espanhola, Corpo Nacional da Polícia Espanhola, Força Policial de Malta, EUROPOL - Centro Europeu de Cibercrime (EC3), UNICEF Espanha, FAPMI ECPAT Espanha, EU KIDS ONLINE. (2021). Grupo de trabalho para a sensibilização, projeto 4NSEEK. Abuso e exploração sexual de menores online: uma análise da 4NSEEK [Pôster]. Léon, Espanha: INCIBE.

International Organization for Standardization. (2005). ISO/IEC 17025:2005.

Internet Watch Foundation (IWF). (2012). *Internet Watch Foundation Annual and Charity Report 2012*. https://www.iwf.org.uk/media/uh1gbzae/2012-annual-report.pdf

Internet World Stats. (2023). Estatísticas mundiais da Internet. Consultado a 30 de junho de 2023. https://www.internetworldstats.com/stats.htm?ref=vc.ru

ISO/IEC 17025:2005, General requirements for the competence of testing and calibration laboratories (2005).

ISO/IEC 23037:2012, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (2012).

ISO/IEC 27032:2012. Information technology - Security techniques - Guidelines for cybersecurity, International Standards Organization (2012).

Lambelho, A. (2022). Algumas considerações sobre a utilização da prova digital em Direito do Trabalho. Revista Jurídica Portucalense, Nº Especial (Vol II), 22-37. https://doi.org/10.34625/issn.2183-2705(ne2v2)2022.ic-02

Leadbeater, C. (1999). *Living on Thin Air: The New Economy.* Viking.

Lei n.º 109/2009, de 15 de setembro. Diário da República n.º 179/2009, Série I de 2009-09-15.

Lei n.º 32/2008, de 17 de julho. Diário da República n.º 137/2008, Série I de 2008-07-17, páginas 4454 - 4458.

Lei n.º 41/2004, de 18 de agosto. Diário da República n.º 194/2004, Série I-A de 2004-08-18, páginas 5241 - 5245.

Lei n.º 49/2008, de 27 de agosto. Diário da República n.º 165/2008, Série I de 2008-08-27.

Lei n.º 53/2007 de 31 de agosto. Diário da República n.º 168/2007, Série I de 2007-08-31, páginas 6065 - 6074.

Lessig, L. (1999). *Code and Other Laws of Cyberspace* (1ª ed.) Basic Books. https://lessig.org/images/resources/1999-Code.pdf

MacKuen, M. B., & Erikson, R. S., & Stimson, J. A. (1992). Peasants or bankers? The American electorate and the U.S. economy. *American Journal of Political Science, 86*, 597-611.

Magalhães, T. (2016). Abuso sexual infantil. In *Dicionário: Crime, Justiça e Sociedade.* (1.ª ed). Lisboa, Portugal: Edições Sílabo, Lda. ISBN 978-972-618-853-7.

Magriço, M. E. (2012). *A exploração sexual de crianças no Ciberespaço - aquisição e valoração de prova forense de natureza digital* [Dissertação de Mestrado]. Academia Militar. https://comum.rcaap.pt/bitstream/10400.26/6822/1/DISSERTACAO-EXPLORACAO-SEXUAL-CRIANCAS-CIBERESPACO.pdf

Marques, P. (2013). *Recolha e preservação da prova digital.* [Dissertação de Mestrado] Faculdade de Engenharia da Universidade Católica Portuguesa. https://repositorio.ucp.pt/bitstream/10400.14/13191/1/13191.pdf

Martins, J. M. (2019). Documentos eletrónicos e meios de prova. In Cordeiro, A. M. (coord.), *Código civil - livro do cinquentenário* (Vol I. - p. 795-824). Edições Almedina.

Martins, M. (2012). Ciberespaço: uma Nova Realidade para a Segurança Internacional. *Revista Nação e Defesa*, *133 (5)*, 32-49.

McLeod, J. (1997). *Narrative and Psychotherapy*. London: Sage

McLuhan, M. (1964). *Understanding Media: The Extensions of Man.* https://designopendata.files.wordpress.com/2014/05/understanding-media-mcluhan.pdf

Mesquita, P. D. (2010). *Processo Penal, Prova e Sistema Judiciário* (1ª ed.). Coimbra Editora.

Ministério da Admnistração Interna. (2022). *Relatório Anual de Segurança Interna.* https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2022-

Ministério Federal do Interior (2021). Estratégia de Cibersegurança da Alemanha. [PDF] https://ccdcoe.org/uploads/2018/10/Germany_cyber-security-strategy-2021_English.pdf

Moraes, F. D. (2013). Ciberespaço entre as redes e o espaço geográfico:algumas considerações teóricas. *Caminhos de Geografia, Uberlândia 14*(47), p. 139-149.

Moreira, J. (2023). *Evolução e Desafios Futuros do Ciberespaço.* X Curso de Cibersegurança e Gestão de Crises no Ciberespaço, Lisboa, Portugal.

Morgado, S. M. A., Carvalho, M., & Felgueiras, S. (2024). Diagnosis model for detection of e-threats against soft-targets. In A. Rocha, H. Adeli, G., Dzemyda, F., Moreira, and V. Colla (eds). Information Systems and Technologies. WorldCIST 2023. Lecture Notes in Networks and Systems, vol 800 (pp. 249–262). Springer, Cham. https://doi.org/10.1007/978-3-031-45645-9_24

Mueller, M., Mathiason, J. & McKnight, L. (2004). Making Sense of "Internet Governance": Defining Principles and Norms in a Policy Context. Internet Governance Project. https://www.wgig.org/docs/ig-project5.pdf

Ning, H., & Ye, X. & Bouras, M. A. & Wei, D. & Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *IEEE Internet of Things Journal*, (V. 5, Nº. 3), 1843-1856. DOI: 10.1109/JIOT.2018.2815535.

NIST. (2013). Glossary of Key Information Security Terms. NISTIR 7298 Revision 2, https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

Nunes, P. (2010). Mundos virtuais, riscos reais: fundamentos para a definição de uma Estratégia da Informação Nacional. *Revista Militar* (Nº 2506), 1169-1198. https://www.revistamilitar.pt/artigo/608

Nye, J. (2010). *Cyber Power* (1ªed.). Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Oliveira, A. (2017). *Acervo Schengen e segurança europeia: a crise de migrantes como ameaça à liberdade de circulação na União Europeia.* ISCPSI.

Oliveira, A. (2020). A pandemia e a transformação digital. *Ingenium*, 54-55. http://web.tecnico.ulisboa.pt/arlindo.oliveira/Ingenium_COVID_article.pdf

Organização das Nações Unidas (ONU). (2017). *Manual de Política de Segurança.* https://www.un.org/en/pdfs/undss-unsms_policy_ebook.pdf

Organização das Nações Unidas. (1989). *Convenção sobre os Direitos das Crianças.* Comité Português para a UNICEF. https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf

Organização das Nações Unidas. (2000). Protocolo Facultativo à Convenção sobre os Direitos da Criança Relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/protocolo_facultativo_convencao_direitos_crianca_venda_criancas-pornog_infantil.pdf

Parlamento Europeu. (2021). Ilustração da sessão do Parlamento Europeu [Imagem]. Biblioteca do Parlamento Europeu. Consultado a 20 de junho de 2023. https://www.europarl.europa.eu/resources/library/images/20210215PHT97846/20210215PHT97846_original.jpg

Pimentel, L. (2020). Da Perícia na Investigação Criminal: Aos Limites da Identificação Judiciária Lofoscópica e Fotográfica. Politeia Ano XVII – 2020, 103-125. https://comum.rcaap.pt/bitstream/10400.26/39622/1/Da%20per%C3%ADcia%20na%20Investiga%C3%A7%C3%A3o%20Criminal%20_Aos%20Limites%20da%20Identifica%C3%A7%C3%A3o....pdf

Pinho, A. L. (2022). Ciberdefesa, Ciberdissuasão e Poder Nacional no Ciberespaço. *IDN Brief, Segurança e Defesa no Ciberespaço*, 2-3. https://comum.rcaap.pt/bitstream/10400.26/42136/1/PINHOAlexandre_SegurancaedefesadociberespacoIDNBrief_Julho_2022.pdf

Polícia Judiciária (2022). Concurso para admissão de 70 candidatos ao curso de formação de inspetores. Prova escrita de conhecimentos específicos.

Prado, G. (2021). *A interface entre o Direito Digital e o Processo Penal* [Comunicação oral]. Ciclo Permanente de Palestras com o tema "Consequências do Uso da Inteligência Artificial no Processo Penal", Lisboa, Portugal.

Presidência do Conselho de Ministros. (2013) Quadro Estratégico Nacional para a Segurança do Ciberespaço. [PDF] https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

Ramos, A. D. (2014). *A Prova Digital em Processo Penal: O Correio Eletrónico* (1ª ed.). Chiado Editora.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Regulamento (UE) Nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014.

Rheingold, H. (1993). *The virtual community: Homesteading the electronic frontier.* New York: Harper Perennial.

Ribeiro, I. (2022). *Tráfico de menores para fins de exploração sexual: Algumas considerações a propósito do lenocínio e do recurso à prostituição de menores.* Faculdade de Direito da Universidade de Coimbra. [Dissertação de Mestrado]. https://estudogeral.uc.pt/bitstream/10316/103643/1/Disserta%c3%a7%c3%a3o%20-%20pdf.pdf

Rigby, K. (1995). Anonymity on the internet must be protected. *Ethics and Law on the Electronic Frontier.* https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.html

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

Rodrigues, B. S. (2011). *Da Prova Penal, Tomo IV, Da Prova - Electrónico-Digital e da Criminalidade Informático-Digital* (Contributo Para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa) (1ª ed.). Rei dos Livros.

Santos, M. (1994). *A observação Científica*. Faculdade de Psicologia e Ciências da Educação da Universidade do Porto https://repositorio-aberto.up.pt/bitstream/10216/54055/2/44387.pdf

Storage of Network Association (SNIA)(2023). What is NAS (Network Attached Storage) and why is NAS Important? Consultado a 3 de janeiro de 2024. https://www.snia.org/education/what-is-nas

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

Suler, J. & Phillips, W. (1998). The Bad Boys of Cyberspace: Deviant Behavior in a Multimedia Chat Community. *Cyberpsychology & behavior: the impact of the Internet, multimedia and virtual reality on behavior and society 1(3),* 275-294 10.1089/cpb.1998.1.275

Toffler, A. (1980). *The Third Wave.* Bantam Books. http://era.gov.kh/eraasset/uploads/2020/02/Toffler.Alvin_.The_.Third_.Wave_.pdf

Tonini, P. (2010). Nuovi profili processuali del documento informatico. In Luisella, D. C., *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica* (pp. 427-445). CEDAM.

Trachtman, J. (1998). Cyberspace, Sovereignty, Jurisdiction, and Modernism. *Indiana Journal of Global Legal Studies, V. 5*(Nº2), 561-581. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1134&context=ijgls

Tribunal de Contas Europeu. (2019).Desafios a uma política de Cibersegurança eficaz da UE https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

União Europeia. (2011). Diretiva n.º 2011/92/UE do Parlamento Europeu e do Conselho de 13 de Dezembro de 2011 relativa à avaliação dos efeitos de determinados projetos públicos e privados no ambiente [PDF]. EUR-Lex. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093

United Nations Office on Drugs and Crime (UNODC). (2009). Modelo de Legislação contra o Tráfico de Pessoas. Nº E.09.V.11 ISBN 978-92-1-133674-0 https://www.unodc.org/documents/human-trafficking/Model_Law_against_TIP.pdf

Urinov, B. N. (2020). Theoretical aspects of organizational behavior and corporate culture. *Economics and Innovative Technologies 2020* (Nº 2), 1-8.

Urry, J. (2000). *Sociology Beyond Societies: mobilities for the twenty-first century* (1ª ed.) Routledge. Sociology beyond Societies: Mobilities for the twenty-first century

Valente, M. M. (2019). *Cadeia de Custódia da Prova* (4ª ed.). Edições Almedina.

Vales, T. P. (2020). *As Contribuições do Ciberespaço para os processos de securitização e dessecuritização* [Dissertação de Doutoramento]. Faculdade de Economia da Universidade de Coimbra. https://estudogeral.uc.pt/bitstream/10316/95266/4/TiagoVales_As%20Contribui%C3%A7%C3%B5es%20do%20Ciberespa%C3%A7o%20para%20os%20processos%20de%20

securitiza%C3%A7%C3%A3o%20e%20dessecuritiza%C3%A7%C3%A3o%20%282%29.pdf

Wang, M-F., Ning, Yue-M. (2002). The Urban Geography of Cyberspace: review and prospect. *Advances in Earth Science,, Vol 17* (6), pp. 855-863. http://www.adearth.ac.cn/EN/10.11867/j.issn.1001-8166.2002.06.0855

We are Social (2023) Digital 2023: Global Overview Report. Janeiro. Digital 2023 - We Are Social UK

We are Social (2023) Digital 2023: Local Country Headline Report. Janeiro. Digital 2023: Local Country Headlines Report — DataReportal – Global Digital Insights

Webster, F. (2002). *Theories of the information society* (3ª ed.). Routledge https://cryptome.org/2013/01/aaron-swartz/Information-Society-Theories.pdf

World Economic Forum (2022). *Global Risks Report 2022: 17h Edition.* https://wef.ch/risks22

WSIS. Declaration of Principles Building the Information Society: a global challenge in the new Millennium (2003). Geneva. Retrieved from http://www.itu.int/net/wsis/docs/geneva/official/dop.html

Zenebe, A., Shumba, M., Carillo, A. & Cuenca, S. (2019). Cyber Threat Discovery from Dark Web. *EPiC Series in Computing, 64,* 174 - 183.

APÊNDICES

APÊNDICE A

Tipos de Dispositivos para recolha de prova digital

Outros dispositivos eletrónicos	● *Personal digital assistants* (computadores portáteis, agendas eletrónicas ou smartphones); ● Equipamentos vídeo (câmara vídeo, gravador de vídeo (VCR) ou leitor); ● Gravadores Áudio; ● *Chips*; ● *Circuit boards*; ● Drones; ● Câmaras digitais; ● Tokens de acesso (*Smart cards*; o Dongles (*security* dongle); *Scanners* Biométricos) ● Telefones; ● Atendedores automáticos; ● Máquinas de Fax; ● Gravadores de voz; ● *Pagers*; ● Playstations com cartões de memória ou discos, Xboxes ou outras consolas de jogos; ● Dispositivos de GPS; ● Relógios Digitais; ● Leitores de bandas magnéticas; ● Fotocopiadoras.
Dispositivos de armazenamento Digital	● Disquetes; ● Backups (i.e., tapes ou DATs); ● Disquetes JAZ, ZIP e ORB; ● CDs e DVDs; ● Discos rígidos não ligados ao computador; ● Placas para PCs; ● Cartões de fita magnética; ● Cartões de memória; ● Pens/keys/sticks USB; ● Dongles; ● Discos Solid State; ● PDA.

Fonte: Adaptado de Marques (2013).

APÊNDICE B

Vantagens e riscos associados aos dois tipos de recolha de prova digital

	Recolha de dispositivos e meios de armazenamento digital	Recolha direta da informação contida nos dispositivos digitais[55]
Vantagens	● Pode ser executada com alguma facilidade por pessoas com formação básica na área da preservação e recolha de equipamentos e meios de suporte de informação; ● Permite operações mais rápidas, o que pode ser vantajoso em ambientes hostis; ● A prova digital fica integralmente preservada; ● Permite posterior pesquisa forense mais cuidada, em ambiente próprio e com ferramentas forenses próprias;	● Não há necessidade de recolha do equipamento, logo, sem prejuízo para o normal funcionamento do local de trabalho; ● O risco de danificar os dispositivos digitais é diminuto.
Riscos	● Risco de danificar os equipamentos e contaminar a própria prova digital; ● Risco de danos colaterais, prejudicando terceiros que nada tenham a ver com os factos em investigação e que se vêm privados dos dispositivos digitais ou dos serviços por estes disponibilizados; ● Risco de prejuízo de outras atividades não relacionadas com os factos em investigação.	● Eventual necessidade da presença de pessoal com formação específica; ● Necessidade de ferramentas forenses de recolha de prova digital (criação de imagens dos discos rígidos e arquivos, tráfego de rede, etc.) ● Eventual necessidade da colaboração do suspeito ou do administrador do sistema; ● Possibilidade de perda da prova original, no caso de "backups" danificados, incompletos ou desatualizados; ● Necessidade de replicar o ambiente do sistema informático alvo, para que o restauro tenha sucesso, nomeadamente com motores da base de dados, programas de gestão documental ou sistemas *Enterprise resource planning*[56](ERP), que se podem revelar demasiado dispendiosos.

Fonte: Manual Técnico de Preservação e Recolha da Prova Digital na Investigação Criminal da Polícia de Segurança Pública (2015).

[55] Ressalva-se que o pessoal da Polícia de Segurança Pública da Polícia Técnica Forense, em especial neste tipo de recolha, deverá avaliar devidamente os riscos e a sua responsabilização.

[56] Sistema de informação que integra todos os dados e processos de uma organização num único sistema.

APÊNDICE C

Dados informáticos passíveis de serem obtidos, por equipamento

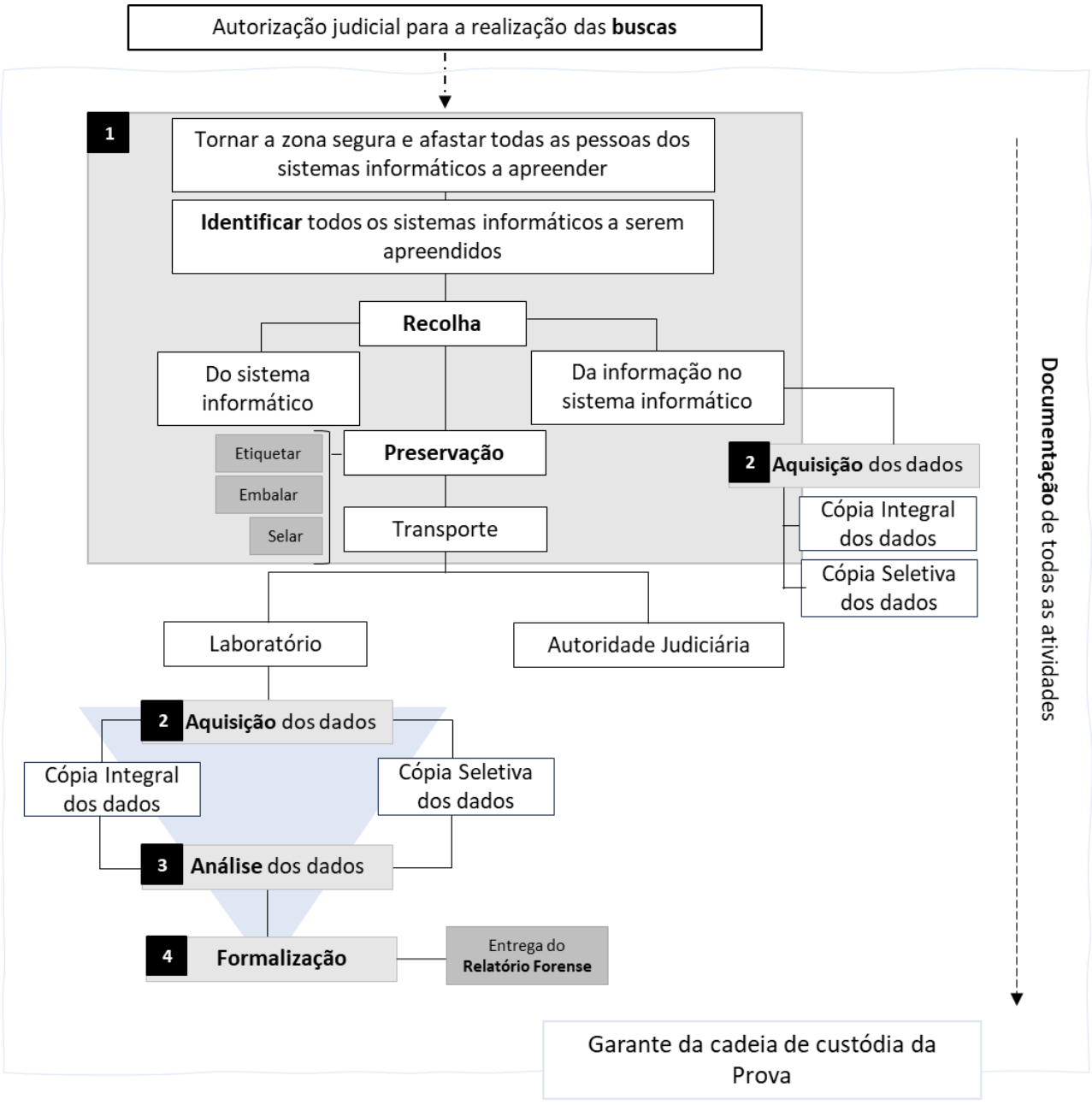
Equipamento	**Dados passíveis de serem obtidos**
Computador	• Histórico de utilização • Histórico de internet • Metadados • Vídeos e imagens • Recuperação de arquivos eliminados • Dados voláteis [RAM e cache] • Correio eletrónico • Dados da nuvem
Telemóvel	• Registo de chamadas • Dados de aplicações [redes sociais, monitorização remota, etc..] • Mensagens SMS e MMS • Vídeos e imagens Correio eletrónico • Dados da nuvem Informações GPS • Histórico de internet
Veículo Automóvel	<u>Dados das Unidades de Controlo Eletrónico (ECU) via OBDII:</u> • Velocidade do veículo • Aceleração brusca • Travagem brusca • Ocorrências do airbag • Uso do cinto de segurança • Abertura de portas • Odómetro <u>Sistemas de infoentretenimento e telemática</u>: • Navegação GPS • Pontos de rastreamento • Conectividade USB e Bluetooth • Contactos • Mensagens SMS e MMS • Registo de chamadas • Histórico de internet • Ficheiros multimédia
Cartão SIM	• Registo de chamadas • Mensagens SMS e MMS

Drone	• Informações recebidas através de sensores • Vídeos e imagens • Comunicações de voz e vídeo • Localização e navegação
CCTV	• Vídeos • Registos de acesso

Fonte: Manual Técnico de Preservação e Recolha da Prova Digital na Investigação Criminal da Polícia de Segurança Pública (2015).

APÊNDICE D

Fluxograma demonstrativo das principais fases do processo de análise digital forense



Legenda:

Perícia Digital Forense

ANEXOS

ANEXO A

Modelo de registo da Cadeia de Custódia em uso da PSP

POLÍCIA SEGURANÇA PÚBLICA

DIREÇÃO NACIONAL
Departamento de Investigação Criminal
Laboratório de Criminalística e Ciência Forense
Secção Digital Forense

CADEIA DE CUSTODIA

PROCESSO:	
COMANDO:	
SUBUNIDADE:	

DISPOSITIVO / DETALHES

Item / Identificador n.º:	**Descrição:**		
Marca:	**Modelo:**	**N.º Serie / IMEI / ICCID**	**Cor:**

DETALHES SOBRE A IMAGEM DOS DADOS

Hora/ Data:	**Criado por:**	**Método usado:**	**Nome imagem:**	**Volumes:**
Dispositivo der armazenamento:	**Código Hash:**			

Origem			**Destino**			**Obs**
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		

Departamento de Investigação Criminal
Quinta das Águas Livres, Belas - Sintra
2605-197 Belas
PORTUGAL

T: +351 218 111 000 - Ext. 12616
F: +351 219 809 823
E: sdf.dic@psp.pt

ANEXO B

Glossário Gráfico dos sacos utilizados pela PSP para acautelar Prova Digital

Saco de Prova		
Saco Anti-Estático		
Saco *Faraday*		

Selo de Segurança			

ANEXO C

Relatório Forense em uso da PSP

POLÍCIA SEGURANÇA PÚBLICA

DIREÇÃO NACIONAL
DEPARTAMENTO DE INVESTIGAÇÃO CRIMINAL
LABORATÓRIO DE CRIMINALÍSTICA E CIÊNCIA FORENSE
SETOR DIGITAL FORENSE

RELATÓRIO FORENSE
Nº 2023-XXX-SDF-DIC/DN

REQUERENTE:
OPC:
NUIPC Nº:
TIPOLOGIA CRIMINAL:
MATERIAL RECEBIDO EM:
EXAME INICIADO EM:
EXAME TERMINADO EM:

I PARTE

1. MATERIAL / EQUIPAMENTO PARA [EXAME, PERICIA FORENSE, ou PESQUISA INFORMÁTICA]

A. Tipo de equipamento:

Item A1 SSD/HDD		Marca: Modelo: Número de serie: Capacidade de armazenamento:	XXX XXX XXX XXX
Item A2 Telemóvel	 Item A2.1 Item A2.2	Marca: Modelo: IMEI: Cartão SIM: Cartão memória	XXX XXX XXX XXX xxx

2. OBJECTO DO EXAME FORENSE / QUESITO (S)

A. Ordem de exame: Autoridade Judiciária, Ministério Público

B. Quesitos do exame (objetivos): extração e pesquisa de dados informáticos, conforme Despacho Judicial.

C. Local do exame forense: Setor Digital Forense do Laboratório de Criminalística e Ciência Forense, do Departamento de Investigação Criminal da PSP.

D. Quem executa:

E. Reprodução fotográfica dos equipamentos indicado em 1.

Departamento de Investigação Criminal
Laboratório de Criminalística e Ciência Forense
Setor Digital Forense

Quinta das Águas Livres, Belas - Sintra 2605-197 Belas
Tel.: 218111000 Ext. 12616 *Fax: 219809823*
e-mail: sdf.dic@psp.pt

3. FERRAMENTAS USADAS NA INTERVENÇÃO TÉCNICA FORENSE

A. UFED® Touch 2: Versão xxx

B. Cellebrite Physical Analyzer®: Dongle serial xxxx

C. MSAB XRY®

D. MSAB XAMN®

E. Tableau TD3, s/n 000ecc01d390a7

F. Opentext Encase

G. Computador com Microsoft Win10 PRO.

Departamento de Investigação Criminal
Laboratório de Criminalística e Ciência Forense
Setor Digital Forense

Quinta das Águas Livres, Belas - Sintra - 2605-197 Belas
Tel.: 218111000 Ext. 12616 *Fax: 219809823*
e-mail: sdf.dic@psp.pt

II PARTE

4. OBSERVAÇÕES E ENSAIOS REALIZADOS

4.1 - Requisitos prévios

4.1.1 - Do pedido de exame

- A autorização legal foi ordenada judicialmente pela Autoridade Judiciária competente e especificamente para a peritagem ao equipamento em ambiente de laboratório.

4.1.2 - Preparação da imagem digital da evidência

- Os sistemas informáticos foram examinados e fotografados;
- Para a pesquisa, análise e cópia parcial dos dados, com base nos critérios de pesquisa indicados pela investigação, foi utilizado o equipamento forense indicado no ponto 3.

4.2 - Processamento técnico forense

Conforme Despacho Judicial foram realizadas as ações nos equipamentos eletrónicos:

4.2.1 Exame e análise aos equipamentos eletrónicos

Item A1 – XXX:

I. Ferramenta forense utilizada para a realização da cópia:
   - Tableau TD3, (descrito em 3.E), com bloqueador de escrita.

II. Disco de cópia – destino de Item A1:
   - Marca: XXX;
   - Modelo: XXX;
   - N.º série: *XXX;*
   - Capacidade: XXX.

III. O processo de criação da imagem completa do disco e de todo o seu conteúdo, incluindo as partições e sectores de arranque, iniciou em XX de XXXXX XXXX, XX:XX e foi concluído com sucesso em XX de XXXXX XXXX, XX:XX.

IV. Foram gerados valores hash (SHA-1) pelo equipamento de cópia do disco:
   - SHA-1: XXXX.

V. Os dados informáticos foram analisados e pesquisados com recurso à aplicação informática OpenText EnCase (Ponto 3.F), seguindo os critérios de pesquisa indicadas pela investigação.

VI. Os resultados obtidos ficaram guardados na pasta \A1_JIC\, cujo relatório é acedido através do ficheiro Item A1.html.

Item A2 – XXX:

- Em xx de xxxxx de xxxx o telemóvel XXXX foi ligado ao equipamento UFED® (ponto 3.A), através do qual foi realizada a extração física dos dados informáticos de conteúdo.
- Em xx de xxxxx de xxxx o Cartão SIM MEO xxxx foi ligado ao equipamento UFED® (ponto 3.A), através do qual foi realizada a extração lógica dos dados informáticos de conteúdo.
- Com base nos critérios de pesquisa e com recurso à aplicação forense UFED Physical Analyzer (ponto 3.B.) foi realizada a análise aos dados informáticos obtidos das extrações, que ficou registada em relatório na pasta Item A1\ nos formatos digitais .xls, .html e .ufdr.
- Com base nos critérios de pesquisa e com recurso à aplicação forense UFED Physical Analyzer (ponto 3.B.) foram extraídos os dados informáticos **de mensagens de aplicações de conversação [chat], mensagens de correio eletrónico [email] e mensagens instantâneas não lidas [SMS],** guardados em suporte de armazenamento autonomo [JIC], na pasta Item A1_JIC\ nos formatos digitais .pdf, e .ufdr.

5. CONCLUSÃO

Solicitado o exame, ao Departamento de investigação criminal, pela Autoridade Judiciária – Ministério Público, foram cumpridos todos os formalismos e imperativos legais, conforme supra se mencionou.

Neste conspecto, quanto aos objetos de exame, em referência, baseada nos critérios de pesquisa fornecidos, foram extraídos dos sistemas informáticos os seguintes dados informáticos:

Item A1 – XXX

Item A2 – XXX

6. DOCUMENTAÇÃO

A. Relatório Forense – relato de todas as ações, processos, resultados e conclusões obtidas.

B. Suporte de armazenamento, **SELADO**, o qual contêm:

- Relatório produzido, com os respetivos ficheiros anexos.
- Folha de suporte, com fotogramas do(s) sistema(s) informático(s).

C. Cadeia de custódia dos sistemas informáticos

Lisboa, XX de XXXX de XXXX

Os Peritos,

_____	_____
xxx	xxx
xxxx	xxxx

ANEXO D

Registo da Cadeia de Custódia em uso da PSP para o Iphone 7

POLÍCIA SEGURANÇA PÚBLICA

DIREÇÃO NACIONAL
Departamento de Investigação Criminal
Laboratório de Criminalística e Ciência Forense
Secção Digital Forense

CADEIA DE CUSTODIA

PROCESSO:	1241/23.1 PP AMD
COMANDO:	COMETLIS
SUBUNIDADE:	DIV/AMADORA/EiC

DISPOSITIVO / DETALHES

Item / Identificador n.º:	Descrição: Telemovél		
Marca: Apple	Modelo: Iphone 7 (A1778)	N.º Serie / IMEI / ICCID 355319088407841	Cor: Branco

DETALHES SOBRE A IMAGEM DOS DADOS

Hora/ Data:	Criado por:	Método usado:	Nome imagem:	Volumes:
Dispositivo der armazenamento:		Código Hash:		

Origem					Destino	Obs
EiC AMADORA	Data: 25/09/2023	Nome/Org.: Margarida	Data: 26/09/2023	Nome/Org.: Lourenço	DN/DCC SDF	
	Hora: 17h03	Assinatura:	Hora: 11h57	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		
	Data:	Nome/Org.:	Data:	Nome/Org.:		
	Hora:	Assinatura:	Hora:	Assinatura:		

Departamento de Investigação Criminal
Núcleo de Polícia Técnica Forense
Seção Digital Forense

Quinta das Águas Livres, Belas - Sintra 2605-197 Belas
Tel.: 218111000 Ext. 12440 Fax: 219809823
e-mail: sdf.dic@psp.pt

ANEXO E

Figura 30. Registo fotográfico do telemóvel “Iphone 7” da marca “Apple”

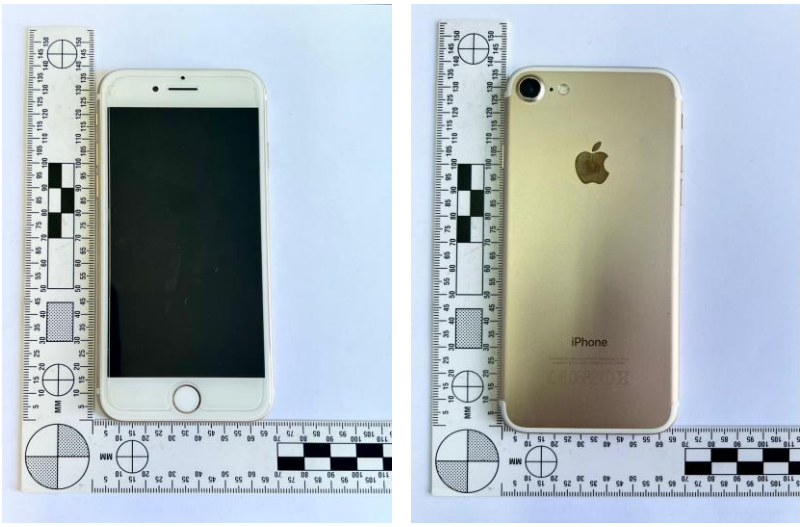
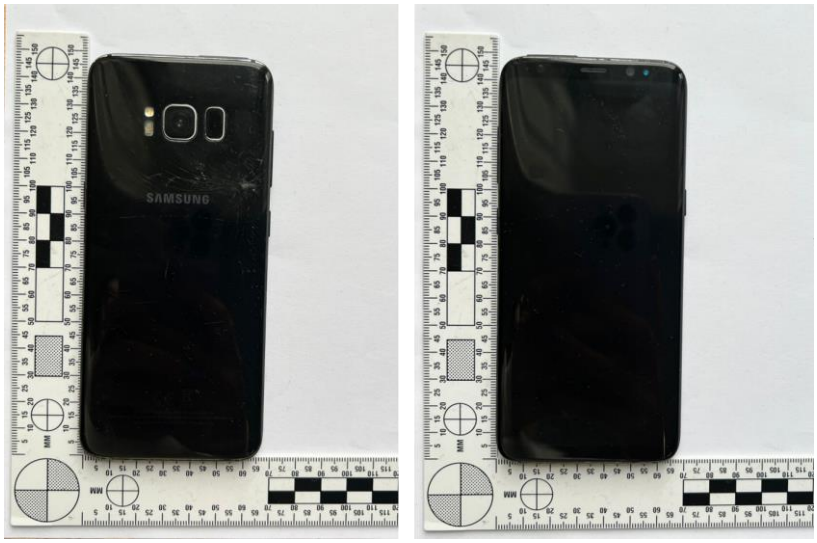


Figura 31. Registo fotográfico do telemóvel “Galaxy S8” da marca “Samsung”



ANEXO F

Autorização para a realização do estágio curricular

POLÍCIA SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
DIRECÇÃO DE ENSINO
SECRETARIA ESCOLAR

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

C/C:
Exmo. Senhor
Diretor do Departamento de Investigação Criminal
DN/PSP Largo da Penha de França, N.1
1199-010 LISBOA

Sua Referência:
Sua Comunicação:
Nossa Referência: 157/SECDE/2023
Classificador: 080.01.10
Processo: SECDE202100002MNI
Data: 2023-07-31

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

1. A Mestranda - Margarida Nunes Carvalho, é aluna do segundo ano do Mestrado em Ciências Policiais na especialização em Gestão da Segurança, encontrando-se a desenvolver a dissertação de Mestrado com o tema: Desafios no Diagnóstico de E-Ameaças, sob a orientação do Superintendente Sérgio Felgueiras.

2. A Mestranda, no âmbito do estudo, vem requerer autorização para a realização de um estágio curricular no Departamento de Investigação Criminal da PSP, laboratório de Criminalística e Ciências Forenses, com o objetivo de solidificar a componente teórica do trabalho.

3. O estágio pretendido seria de 6 meses com início previsto no mês de setembro a março de 2024.
4. Assim, envia-se a V. Ex.ª o requerimento para decisão superior.

O Diretor

José Carlos Bastos Leitão
Superintendente-Chefe

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

137112
Pagina1/1