Instituto Superior de Ciências Policiais e Segurança Interna

Micaelo dos Santos Reis Nabais
Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXV Curso de Formação de Oficiais de Polícia

Agente encoberto:

(in)admissibilidade da prova obtida em ambiente digital

Orientadores:

Professora Doutora Maria Fernanda Palma

Prof. Dr. Rui Carlos Pereira

Lisboa, 15 de maio de 2023

Instituto Superior de Ciências Policiais e Segurança Interna

Micaelo dos Santos Reis Nabais
Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXV Curso de Formação de Oficiais de Polícia

Agente encoberto:

(in)admissibilidade da prova obtida em ambiente digital

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna, com vista à obtenção do grau de Mestre em Ciências Policiais, elaborada sob orientação científica da Professora Doutora Maria Fernanda Palma e do Prof. Dr. Rui Carlos Pereira.

Lisboa, 15 de maio de 2023

Estabelecimento de Ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Curso:	XXXV
Orientação científica:	Professora Doutora Maria Fernanda Palma Prof. Dr. Rui Carlos Pereira
Título:	Agente encoberto: (in)admissibilidade da prova obtida em ambiente digital
Autor:	Micaelo dos Santos Reis Nabais
Local de Edição:	Lisboa
Data de Edição:	15 de maio de 2023

Dedicatória

À minha mãe, *in memoriam*.

Ao meu pai.

Agradecimentos

Na semana em que entreguei o projeto relativo a esta investigação faleceu a minha mãe, subitamente. A sua partida inesperada deixou um vazio incomensurável no meu coração. Sendo ela a força motriz que me incentivou a iniciar e permanecer neste curso, por sempre ter acreditado em mim, nada menos poderia dar-lhe do que colocar a sua presença e amor em cada página deste trabalho. O meu pai, apesar de toda a dor sentida, tem sido incansável para comigo em todos os aspetos. Espero conseguir retribuir em igual medida. Obrigado, mãe. Por tudo o que fizeste por mim até ao último dia da tua vida. Obrigado, pai. Por tudo o que continuas a fazer.

Agradeço aos meus orientadores, por confiarem no meu projeto, pelo privilégio que me deram, pelo tempo despendido, por toda a ajuda, sempre que solicitada.

Deixo uma palavra de gratidão aos professores que tive ao longo deste curso. Seguramente influenciaram o meu crescimento pessoal e profissional.

Por vezes surgem dificuldades que parecem insuperáveis, no entanto, com o apoio dos que em nós acreditam, através de colaboração mútua, o sucesso torna-se mais tangível. Este trajeto que agora finda não foi exceção. Agradeço à Ana Duarte, ao Daniel Ferreira, ao Diogo Santos, ao Hélder Vilaverde, à Paula Faria, ao Mamadi Dafé, à Mariana Azevedo e ao Samuel Rosário pela amizade que com cada um construí. Após enfrentarmos alguns obstáculos juntos, aproxima-se o momento de celebrarmos, igualmente juntos.

Durante os últimos 5 anos tive a oportunidade de conviver com alunos desde o XXXI ao XXXIX CFOP´s. Acumulei memórias de momentos felizes, partilhados de forma transversal um pouco por todos os cursos, o que me enche de satisfação. Deixo uma palavra de apreço aos camaradas que ao longo deste período não terminaram os respetivos cursos, fazendo votos para que a experiência lhes tenha aberto outros horizontes, igualmente nobres.

Quero também lembrar, neste momento, todos os polícias e civis que prestaram serviço no ISCPSI ao longo deste 5 anos, que prestaram serviço na EPP aquando do 9.º CFA, a todos os polícias da Divisão de Castelo Branco com quem trabalhei antes de abraçar este desafio, aos polícias da 4.ª Divisão do COMETLIS, onde também prestei serviço e regressei para estagiar, e ainda aos polícias da Divião de Oeiras, onde também estagiei.

Todos acrescentaram algo à minha vida, cabendo-me a mim fazer o melhor uso possível de todos os ensinamentos e partilha de experiências, pois o maior desafio apenas começa agora.

Epígrafe

"Só se vê bem com o coração.
O essencial é invisível aos olhos."
Antoine de Saint-Exupéry

Resumo

Com a globalização e o advento das novas tecnologias, o sistema penal tem sido desafiado a rever conceitos e questões jurídicas, algumas já amplamente consolidadas na sua aplicabilidade ao mundo físico. Uma dessas questões prende-se com o método oculto de investigação criminal correspondente às ações encobertas, agora em ambiente digital, cujo recurso se torna essencial devido à complexificação da cibercriminalidade. Perante este contexto, a força motriz desta investigação passou por analisar a admissibilidade da prova obtida por meio destas ações no ordenamento jurídico português. Para atingir o desiderato de encontrar resposta para este problema de natureza jurídica, adotou-se uma revisão da literatura sobre o tema, alicerçada no método jurídico e da interpretação do direito, tendo como base a pesquisa por documentação indireta, tanto documental como bibliográfica. De acordo com os dados coletados, concluiu-se que não é clara a admissibilidade da prova obtida em contexto de investigação criminal pelo agente encoberto digital, podendo variar de acordo com a doutrina jurídica e de uma análise casuística pelos tribunais, para além do estrito cumprimento de requisitos legais e constitucionais. Os resultados indicaram que os métodos utilizados no decorrer das ações encobertas digitais seguem ainda a mesma linha dos métodos tradicionais em ambiente físico, porém com adaptações, pelo que urge a necessidade de uma reformulação legal nesta matéria.

Palavras-chave: admissibilidade da prova; ambiente digital; ações encobertas; métodos ocultos de investigação criminal; prova.

Abstract

With globalization and the advent of new technologies, the criminal justice system has been challenged to review concepts and legal issues, some of which are already widely consolidated in their applicability to the physical world. One of these issues relates to the hidden method of criminal investigation corresponding to undercover actions, now in a digital environment, whose use becomes essential due to the complexity of cybercrime. In this context, the driving force of this investigation was to analyze the admissibility of evidence obtained through these actions in the portuguese legal system. To achieve the goal of finding an answer to this legal problem, a literature review was conducted on the topic, based on the legal method and interpretation of the law, based on indirect documentation research, both documentary and bibliographical. According to the data collected, it was concluded that the admissibility of evidence obtained in the context of criminal investigation by the digital undercover agent is not clear, and may vary according to legal doctrine and a case-by-case analysis by the courts, in addition to strict compliance with legal and constitutional requirements. The results indicated that the methods used in digital undercover actions still follow the same line as traditional methods in a physical environment, but with adaptations, which requires the need for legal reform in this matter.

Keywords: admissibility of evidence; digital environment; evidence; hidden methods of criminal investigation; undercover actions.

Lista de siglas e abreviaturas

Ac.	Acórdão
AJ	Autoridade Judiciária
al.	Alínea
Art.º(s)	Artigo(s)
Cap.	Capítulo
CC	Código Civil
CCiber	Convenção sobre o Cibercrime
Cfr.	Conforme
CNPD	Comissão Nacional de Proteção de Dados
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
DCIAP	Departamento Central de Investigação e Ação Penal
Dec.-Lei	Decreto-Lei
e. g.	Por exemplo
EUA	Estados Unidos da América
Europol	*European Union Agency for Law Enforcement Cooperation*
ex vi	Por força
FBI	*Federal Bureau of Investigation*
GNR	Guarda Nacional Republicana
GPS	*Global Position System*
GSM	*Global System for Mobile Communications*
JIC	Juiz de Instrução Criminal
LCiber	Lei da Cibercriminalidade
LSI	Lei de Segurança Interna

MP	Ministério Público
n.º(s)	Número(s)
NIST	*National Institute for Standarts and Technology*
OPC(s)	Órgão(s) de Polícia Criminal
OSINT	*Open Source Intelligence*
p./pp.	Página(s)
PGR	Procuradoria Geral da República
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
PUC-CPI	Ponto Único de Contacto para a Cooperação Policial Internacional
RASI	Relatório Anual de Segurança Interna
RJAE	Regime Jurídico das Ações Encobertas
s./ss.	Seguinte(s)
SEF	Serviço de Estrangeiros e Fronteiras
SIED	Serviço de Informações Estratégicas de Defesa
SIRP	Sistema de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
STJ	Supremo Tribunal de Justiça
TC	Tribunal Constitucional
TCIC	Tribunal Central de Investigação Criminal
TRC	Tribunal da Relação de Coimbra
TRE	Tribunal da Relação de Évora
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto
UE/EU	União Europeia
Vd	Vide

Índice

Introdução

a) Apresentação e delimitação do tema

Estamos a assistir a um desenvolvimento das tecnologias da informação que não tem paralelo. Embora tenham trazido benefícios significativos à sociedade, como o aprimoramento de áreas desde a saúde e bem-estar à economia, passando pelas indústrias, há também um reverso da medalha, na medida em que estas são aproveitadas como ferramentas para o desenvolvimento de uma nova forma de criminalidade.

Assim, estamos agora perante uma criminalidade desterritorializada e sem rostos, que permite aos criminosos realizar os seus intentos atrás dos ecrãs de computadores, *smartphones* ou *tablets*, desde o conforto dos seus lares, ou de outros lugares, principalmente através de redes como a internet. Esta metamorfose criminal tem vindo a ser acompanhada pelas polícias de todo o mundo, de modo a poderem preveni-la e reprimi-la, assim como um pouco por todos os operadores da justiça, pelo que tem havido nos diversos ordenamentos jurídicos alterações neste sentido.

No contexto português, entre outras alterações, fomos reforçados com a Lei n.º 109/2009, de 15 de setembro, denominada por Lei do Cibercrime (LCiber), que transpôs para o âmbito nacional a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre o Cibercrime do Conselho da Europa (CCiber). Esta ferramenta da União Europeia (UE) serviu como resposta ao então novo paradigma da prova digital e ainda para trazer alguma harmonia na regulação dos meios de obtenção de prova neste mesmo âmbito, que não existia.

A LCiber acrescentou, como uma das suas inovações, o fato de no seu Art.º 19.º tornar admissível o recurso às ações encobertas na investigação dos crimes de entre um catálogo nela elencado. Desta feita, o método de investigação criminal relativo às ações encobertas previsto na Lei n.º 101/2001, de 25 de agosto, denominada por Regime Jurídico das Ações Encobertas (RJAE), passou também a ser possível realizar em ambiente digital. Esta figura do agente encoberto tinha surgido anteriormente porque os métodos de investigação tradicionais não eram suficientes para determinados tipos de criminalidade.

As ações encobertas são, de acordo com Palma (2011), uma forma plausível para a investigação criminal em relação a um conjunto de crimes graves, desde que promovidas, autorizadas ou conhecidas pelo Ministério Público (MP) e pelo juiz, e obedecendo a critérios

de adequação e proporcionalidade. Já quanto à figura do agente encoberto em ambiente digital, segundo Ramos (2022), esta revolucionou a forma de investigar dos processos crime, com metodologias e métodos novos, para se chegar à recolha da prova.

Ainda que num sistema jurídico distinto, um caso paradigmático da efetividade da sua aplicação é o dos Estados Unidos da América (EUA), onde, de acordo com Braz (2020, p. 358), se "trata de um meio processual utilizado hoje, muito particularmente no domínio da luta contra o tráfico de estupefacientes, crime pelo qual o recurso a esta técnica de investigação adquiriu, historicamente, maior relevância". Ramalho (2017, p. 281) acrescenta que "os EUA são também pioneiros na utilização do agente encoberto em ambiente digital, nomeadamente nas investigações para a deteção da prática de ilícitos relacionados com pornografia infantil em salas de *chat*", fazendo-o já desde o início dos anos 90 através do *Federal Bureau of Investigation* (FBI).

Valente (2019, p. 616) diz-nos que o agente encoberto digital "cujo rosto e forma não são confirmáveis, visíveis e palpáveis, é portador de um elevado risco para o estado constitucional democrático, cujos valores da lealdade e da democracia se esmiúçam e se esmiolam nas relações de confiança societária". Antunes (2017), acrescenta-nos que qualquer método de obtenção de prova é crucial no que diz respeito à sua validade, para que esta possa ser utilizada em sede de julgamento, com o fim último de se chegar à descoberta da verdade material.

Posto isto, definimos como temas delimitadores desta investigação, *primum*, o estudo da figura do agente encoberto digital previsto na LCiber, cuja aplicação é a prevista, *mutatis mutandis*, no RJAE, seu regime geral, procurando determinar as várias formas de recolha de prova possíveis neste tipo de ações encobertas e respetiva (in)admissibilidade; e, *secundum*, compreender em que moldes está estruturada no ordenamento jurídico a recolha de prova digital, que cremos ser o principal tipo de prova recolhida no decorrer de ações encobertas digitais, uma vez que não existe nem diploma legal específico nem enquadramento próprio no título referente aos meios de obtenção de prova do Código de Processo Penal (CPP).

A presente investigação insere-se na área das ciências jurídicas e do direito, interligando-se com a temática da investigação criminal, e por isso, com pertinência na área das ciências policiais. Acompanhamos, por isso, a conceção de ciências policiais de Elias (2018), para quem estas ciências são o "produto da reflexão, análise e pensamento crítico, da análise e revisão bibliográfica, do cruzamento de teorias e métodos científicos de diferentes áreas do saber" (p. 36).

b) Problema de investigação

No âmbito da realização de um trabalho cientifico o investigador deve procurar estruturar o seu trabalho com coerência, sendo que a primeira fase, de acordo com Quivy e Campenhoudt (2008, p. 32), consiste em "procurar enunciar o projeto de investigação na forma de uma pergunta de partida, através da qual o investigador tenta exprimir o mais exatamente possível o que procura saber, elucidar, compreender melhor". Lakatos e Marconi (2003, p. 86) complementam esta ideia ao afirmarem que "o tema da pesquisa é o assunto do estudo", e Coutinho (2018) finaliza, acrescentando que numa investigação faz-se a formulação do problema por via de uma pergunta.

O trabalho de investigação a que nos propomos tem como finalidade responder àquela que hipoteticamente pode ser uma lacuna no ordenamento jurídico português, na medida em que existe um emaranhado normativo em redor da utilização da figura do agente encoberto digital e respetivas provas por este obtidas.

Posto isto, definimos como pergunta de partida: «No ordenamento jurídico português, é clara a admissibilidade da prova obtida em contexto de investigação criminal pelo agente encoberto em ambiente digital?», e como pergunta derivada: «Qual(ais) o(s) método(s) que permite(m) ao agente encoberto digital obter prova admissível?», às quais procuraremos responder seguindo os objetivos de estudo que elencamos de seguida.

c) Objetivos do estudo

Larenz (1997) refere-nos que os problemas devem ser abordados a partir dos mais diversos ângulos, que tragam à colação todos os pontos de vista, tanto os obtidos a partir da lei como os de natureza extrajurídica. Deste feita, tomaremos em conta todos os fatores imprescindíveis para efetuar uma investigação sólida, de modo a obtermos respostas consistentes.

De acordo com Ramos (2022), a figura do agente encoberto digital acarreta consigo diversos problemas, tais como (a) possíveis proibições de prova, caso não sejam cumpridos todos os formalismos, (b) violar princípios constitucionais, ou ainda, (c) afetar direitos, liberdades e garantias do individuo arguido. Segundo Silva (2020, p. 33), "se o Tribunal não lograr a prova dos fatos que constituem o objeto do processo, deve considerar a acusação não provada e como consequência lógica não aplicar qualquer sanção ao arguido".

Como já sabemos, é possível no ordenamento jurídico português fazer recurso à figura do agente encoberto digital em sede de investigação criminal. Não existe ainda,

contudo, um regime específico para a atuação deste, pelo que se utiliza, ainda que com as adaptações necessárias, as normas plasmadas no regime geral.

Nesta senda, vários são os objetivos inicialmente prognosticados relativamente ao presente estudo, pelo que os densificamos nestes cinco, a saber: *primum*, verificar se, efetivamente, uma norma da LCiber que remete para o RJAE, é quanto baste para que se efetuem ações encobertas num ambiente digital, totalmente diferente do real; s*ecundum*, fazer a delimitação concetual de ambiente digital, de modo a compreender se a aplicabilidade deste termo é correto; *tertium*, apurar, uma vez que esta regulação é difusa, em que moldes se obtém prova digital no ordenamento jurídico; *quartum*, averiguar qual ou quais os *modi faciendi* que podem ser adotados no decorrer das ações encobertas digitais, para se efetuar efetivamente a recolha de prova; e, por fim, *quintum,* apreciar a admissibilidade destes meios de obtenção de prova e respetiva prova por estes obtida no inquérito penal.

d) Método

De acordo com Santo (2015, p. 11) o método é o "caminho de investigação apropriado e validado face a objetivos, meios, resultados esperados da mesma e contexto de implementação, incluindo a definição e operacionalização de conceitos". Lakatos e Marconi (2003), acrescentam que o método equivale ao "conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros -, traçando o caminho a ser seguido, detetando erros e auxiliando as decisões do cientista" (p. 83).

Para Gil (2008), a pesquisa bibliográfica é desenvolvida a partir de material constituído principalmente por livros e artigos científicos. Para este autor, independentemente de em quase todos os estudos ser exigido trabalho desta natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas, a partir da técnica de análise de conteúdo. Segundo Teles (2000), a recolha normativa, doutrinária e jurisprudencial, sujeita a uma análise global, dá a conhecer o seu universo a partir do confronto entre fatos e normas jurídicas, fazendo emergir as lacunas e problemas, e por fim, adicionar a crítica, a verificação das normas, da doutrina e da jurisprudência e relacioná-las com as necessidades e aspirações sociais e doutrinárias. Para Larenz (1997), consistindo o trabalho essencialmente no estudo das normas, não existe necessidade de métodos experimentais ou de observação.

Será utilizado neste trabalho científico o método jurídico e da interpretação do direito, comumente empregue com o fim de solucionar problemas de natureza jurídica. Para

isso, teremos como base a pesquisa por documentação indireta, quer documental, como leis, pareceres e jurisprudência, quer bibliográfica, como livros da especialidade e doutrina existente sobre a temática, - nacional e internacional.

No que concerne à estrutura da presente investigação, consiste a mesma em três capítulos, sendo que será sempre feita a abordagem aos diferentes assuntos desde o geral para o particular. No primeiro capítulo, e ainda numa base de contextualização, pretendemos analisar o atual paradigma do agente encoberto na sua forma tradicional, ou seja, no meio físico, fazendo para tal uma resenha histórica, a delimitação concetual necessária para a compreensão das diferentes figuras semelhantes, assim como o estudo do RJAE e respetivas especificidades técnico-práticas deste método oculto de investigação criminal.

No segundo capítulo estudaremos, por sua vez, o agente encoberto na sua vertente digital, fazendo um introito ao fenómeno da cibercriminalidade, a delimitação concetual daquilo que é o ambiente digital, e o estudo do regime presente na LCiber, que admite as ações encobertas digitais.

Por fim, no terceiro capítulo, abordaremos a importância da prova na investigação criminal, evidenciando a prova digital, respetivas especificidades e o regime jurídico em torno da sua obtenção, assim como analisaremos as várias formas encontradas na doutrina para se obter prova no decorrer das ações encobertas realizadas em ambiente digital, estudando a respetiva admissibilidade, ou não, de cada uma.

Capítulo I. As ações encobertas tradicionais

1.1. Resenha histórica das ações encobertas

É difícil determinar temporalmente o momento em que a figura do agente encoberto surgiu enquanto meio de obtenção de prova no processo criminal, e mais difícil ainda é encontrar o prelúdio das ações encobertas em termos bélicos, económicos ou políticos. Confundindo-se ao longo do tempo a figura do agente encoberto com a do espião, do informador, do infiltrado ou do provocador[1], tem acompanhado desde o início a história da humanidade.

Para Catana (2018), as ações encobertas iniciaram com a necessidade de se espiar secretamente a atividade dos inimigos, com o objetivo de se obterem informações relevantes relativamente à forma como se poderiam defender destes ou atacá-los. Knightley (1990) acrescenta-nos que foram encontradas na Turquia escrituras na argila com mais de 3000 anos, contendo informações detalhadas sobre a localização dos inimigos de um povo denominado por hititas, e que já no Antigo Testamento há referências de Moisés a enviar espiões em missão à antiga cidade de Canaã.

Enquanto método de investigação propriamente dito, as primeiras referências a estas figuras surgiram, para autores como Sanchez (1995), Martins (2003) e Pereira V. (2016), no *Ancien Régime* francês, na segunda metade do século XVI, durante a regência do Reis Luís XIV. Neste período as funções passavam em grande parte pela espionagem de comportamentos dos cidadãos (Pereira V., 2016). De acordo com Silva (2003) era um serviço relevante na medida em que fortalecia o poder do rei com recurso às informações obtidas, podendo este antecipar decisões. Contudo, esta atividade acabou por se tornar insuficiente, pelo que, segundo Sanchez (1995), os agentes tiveram de passar da simples espionagem e recolha de informações para a provocação, organizando e fomentando distúrbios sociais, de modo a criarem um ambiente psicológico tenso no seio da sociedade, propício a justificar as medidas necessárias ao regime absolutista de então.

No apogeu do recurso a esta técnica estima-se que houvessem mais de 3000 agentes só na zona de Paris, havendo tanta complexidade que foram divididos em três grupos com funções distintas, nomeadamente os *observateurs*, *espions* e os *bass-mouches*, ou seja, os observadores, os espiões e os informadores (Fijnaux & Marx, 1995). De acordo com Meireis (1999), a maior parte destes indivíduos provinham das classes mais baixas, incluindo

[1] Vd cap. 1.2., onde delimitaremos as diferenças entre estas figuras.

reclusos, que negociavam a sua liberdade em troca dessa cooperação, uma vez que pertenciam aos ambientes a vigiar. Após a revolução francesa, a polícia local continuou a incluir o recurso a estes indivíduos, que auxiliavam em tarefas tais como combater os jogos de azar, a imprensa clandestina, ou mesmo para se desembaraçarem, a qualquer custo, de sujeitos que incomodavam o bem-estar social, mas para os quais não havia prova suficiente para a condenação (Meireis, 1999).

A França destacou-se relativamente a esta realidade, mas as ações encobertas foram emergindo um pouco por toda a Europa. Na mesma época, utilizava-se a prática do *agent provocateur* a uma larga escala na Espanha, nomeadamente nas atividades da igreja católica relacionadas com a inquisição, havendo agentes que procuravam e identificavam manifestações heréticas, de modo a deterem os envolvidos (Oneto, 2005). Matos (2015, p. 14) destaca mesmo que "o agente provocador tem origem na inquisição e (...) nos regimes onde impera o absolutismo e em governos totalitários".

As ações encobertas surgiram também na Alemanha em 1852, com os objetivos de combater a criminalidade e identificar os opositores do regime político de então, quando a direção da Polícia de Berlim criou o Departamento de Investigação Criminal (*Kriminal Polizei*), e lhes deu essas competências (Pereira V., 2016).

De acordo com Fijnaux e Marx (1995, p. 15), "os legados da União Soviética e do Império nazi desempenharam um papel importante ao nível da expansão das táticas encobertas". No Reino Unido este ímpeto surgiu precisamente durante as grandes guerras, não só devido a estas influências, mas também devido à ineficácia do policiamento uniformizado, que tinha surgido pouco antes, na década de 30 (Ramos, 2022).

As ações encobertas chegaram aos EUA com a criação do *Bureau of Investigation*, precursor do FBI, em 1908, durante a presidência de Roosevelt (Pereira V., 2016). Mais tarde, na segunda metade do século XX, passaram a ser muito comuns com fins de investigação criminal pelas polícias, como recurso a novas técnicas de recolha de prova, principalmente no combate à proliferação do tráfico de estupefacientes perpetrado por organizações criminosas complexas (Silva, 2015). Neste contexto consistia, segundo Silva, (2015), em infiltrar polícias no interior destas organizações, com recurso a identidades fictícias, com o objetivo de desmontar toda a organização, identificando autores, *modi operandi* e fazendo toda a recolha de provas necessária.

Já no século XXI, não só nos EUA, mas um pouco por todo o globo, surge a necessidade de transpor estas técnicas também para o combate ao terrorismo, uma vez que a

capacidade de obtenção de informações úteis no âmbito das investigações de foro criminal, relativamente às organizações terroristas, era insignificante (Costa, 2014).

Em Portugal, os primeiros relatos de ações encobertas remontam a 1603, nomeadamente enquanto espionagem política nas Ordenações Filipinas, e a 1760, quando foi criada a Intendência Geral da Polícia, Corte e Reino, continuando a haver referências da sua utilização no decurso do período absolutista e posteriormente no liberal (Ramos, 2022).

No início do estado novo, o Dec.-Lei n.º 22:992, de 29 de agosto de 1933, criou a Polícia de Vigilância e Defesa do Estado, que logo no seu preâmbulo refere que esta exerce "a função de vigilância político-social". Ao longo do tempo as ações encobertas de cariz político foram efetuadas por este organismo até que em 1945, foi extinto e deu lugar à Polícia Internacional e de Defesa do Estado, pelo Dec.-Lei n.º 35:046, de 22 de outubro de 1945, que continuou as funções de vigilância nos mesmos termos.

Concomitantemente foi criado um novo serviço de segurança, a Polícia Judiciária (PJ), pelo Dec.-Lei n.º 35:042, de 20 de outubro de 1945, cujo preâmbulo nos diz que há "certas formas de atividade criminal para cuja prevenção não basta a simples ação estática de presença, antes exigem aturado trabalho de investigação e ativa vigilância por agentes especializados no conhecimento e dos processos criminais". Para Ramos (2022, p. 33) foram aqui "criados os alicerces para a regulamentação da utilização do agente encoberto em Portugal, que viria a ocorrer nos anos 80".

A figura do agente encoberto tem o seu primeiro vislumbre no ordenamento jurídico português quando o Dec.-Lei n.º 430/83, de 13 de dezembro, habitualmente conhecido como «lei da droga», no seu Art.º 52.º estabelece que "não é punível a conduta do funcionário de investigação criminal que, para fins de inquérito preliminar, e sem revelação da sua qualidade e identidade, aceitar diretamente ou por intermédio de um terceiro a entrega de estupefacientes". Mais tarde este diploma legal é revogado pela Lei n.º 15/93, de 22 de janeiro, mantendo esta conduta como não punível. Posteriormente, a Lei n.º 36/94, de 29 de setembro, atinente às medidas de combate à corrupção e criminalidade financeira, legitimava no seu Art.º 6.º os atos de colaboração ou instrumentais "com vista à obtenção de provas em fase de inquérito (...) relativamente aos crimes previstos no n.º 1 do Art.º 1.º", facultando também aqui a possibilidade de recurso a esta figura no âmbito da investigação criminal.

Terminado este caminho, parece consensual que a utilização das ações encobertas, como forma de obter informações de apoio aos decisores e principalmente enquanto meio de investigação à criminalidade, já existe há bastante tempo e tem sido usada regularmente como técnica policial em vários locais.

Segundo Ramos (2022), foi a proliferação de doutrina e jurisprudência em torno desta temática dos métodos proibidos de prova um pouco por toda a Europa e nos EUA que levou ao surgimento de legislação específica para regulamentar a utilização do agente encoberto.

1.2. Conceito de agente encoberto e delimitação face a outras figuras

Ao longo desta resenha histórica foram vários os nomes dados às ações encobertas, pois o próprio conceito evoluiu de acordo com o contexto social e político a cada momento. Para Ramos (2022), a expressão infiltrado pode ser conotada com o desígnio de se espiar em "ambientes ditatoriais" (p. 56) enquanto encoberto pode sê-lo com a necessidade de uma identidade falsa, devidamente concedida e regulamentada, para se ter acesso a determinados locais de difícil acesso ou vedados a um polícia em funções.

A presente investigação recai sobre a figura do agente encoberto, conforme expressão que é utilizada na lei, no entanto, antes de avançarmos, importa frisar desde já que a doutrina não é consensual relativamente à nomenclatura deste instituto jurídico em que se faz a ocultação da verdadeira identidade para interagir e obter prova junto dos criminosos. Destacamos a evolução de um conceito que se construiu a partir das necessidades de cada contexto, mas que ainda não apresenta doutrina nem jurisprudência consensuais. Posto isto, procuraremos fazer a delimitação dos conceitos de agente encoberto, agente infiltrado, agente provocador, terceiro e ainda do informador, figuras estas que são conotadas para autores como Rodrigues (2011a, p. 389) e Andrade (2009a, p. 107), enquanto "homens de confiança", cuja base concetual para este termo é o acesso a informação privilegiada por via da ocultação da verdadeira identidade.

Para começar, relativamente à dicotomia entre encoberto e infiltrado, Catana (2018) diz-nos que existem duas correntes doutrinárias, uma que aceita ambas as figuras autonomamente e outra que as reduz a uma só (as cited in Alves, 2021).

Tomamos como ponto de partida o fato de o RJAE utilizar os termos "ação encoberta" e "agente encoberto", (e ainda o de "terceiro"), pelo que foi *a posteriori* que a doutrina trouxe à colação diferente terminologia. A jurisprudência utiliza os termos «encoberto» e «infiltrado» de forma indefinida. Devido a essa indefinição, o Parecer do Conselho Consultivo da Procuradoria Geral da República (PGR) n.º I001462001, de 16 de maio de 2002, emitido menos de um ano depois da publicação do RJAE, refere que:

> Considera-se a atuação de agente infiltrado ou encoberto a que é desenvolvida por funcionário de investigação criminal ou por terceiro sob controlo policial, com ocultação da sua qualidade e identidade, para prevenção ou repressão dos crimes abrangidos, mediante autorização prévia de autoridade judiciária.

Oneto (2005) segue esta linha de pensamento e defende que encoberto e infiltrado são a mesma figura, afirmando que "o legislador optou pela expressão agente encoberto ao invés de utilizar o termo agente infiltrado, nela se incluindo a realidade que pode comportar as duas figuras" (pp. 140-141). Acrescenta que qualquer polícia a desempenhar funções trajado à civil, ou à paisana, não é passível logo à partida de ser identificado pelos meliantes, e que se este for abordado por um traficante de droga, tem a obrigatoriedade de o deter em flagrante delito[2]. Reforça a sua tese ao dar o exemplo de um outro polícia que também trajando à civil e perante a mesma situação, mas a efetuar uma operação no âmbito do RJAE, pode e deve retardar o flagrante, de modo a ganhar a confiança dos meliantes envolvidos e obter mais provas.

Ramos (2022) concorda que estas figuras são "sinónimas" (p. 68), dando nota que desempenham uma função de recolha de informação com recurso à obtenção da confiança dos visados. Ramalho (2017) afirma mesmo que a distinção entre encoberto e infiltrado é inútil e gera confusão.

No entanto, outros autores consideram que o agente encoberto e infiltrado são figuras distintas. Destacamos Meireis (1999), para quem o agente encoberto é um polícia, ou terceiro concertado com este, que frequenta algum local conotado com a prática de determinados ilícitos criminais, mas que, no entanto, é totalmente passivo relativamente à conduta dos criminosos, estando apenas a aguardar que o crime aconteça. Ainda o mesmo autor define o agente infiltrado como um agente que tem um "papel mais ativo que o encoberto" (p. 193), mas sem incitar a prática do delito. Desta feita, para o autor a diferença está na intensidade da relação de confiança, que no primeiro caso é nula e no segundo não.

Já para Valente (2019), o agente encoberto não carece de autorização judicial pois não atua diretamente junto dos agentes criminosos, encontrando-se apenas a aguardar o desenrolar da ação e que os crimes ocorram. Assim, o agente encoberto não carece de nenhuma interação pessoal nem de ganhar a confiança, não contribuindo de nenhuma forma

[2] *Ex vi* do Art.º 255º n.º 1 do CPP.

para o *actus* do crime. Segundo este, poderá ser qualquer agente da Polícia de Segurança Pública (PSP) ou da Guarda Nacional Republicana (GNR) nas suas funções de prevenção ou investigação criminal, independentemente de um catálogo de crimes, ficando fora do âmbito do RJAE.

Perante estas duas correntes distintas que abordamos na presente investigação, e com a devida vénia por todos os autores, tendemos a convergir com o defendido por Oneto (2005), Ramalho (2017) e Ramos (2022), pois no nosso entendimento a distinção entre os dois conceitos apenas complexifica a temática. Por este motivo e também por ser o termo utilizado na lei, vamos utilizar ao longo da presente investigação a terminologia «agente encoberto» e «ações encobertas».

O Ac. do STJ n.º 127/10.0JABRG.GS.S1, de 27 de junho de 2012 também vai no sentido das figuras do encoberto e infiltrado serem a mesma, separando-as isso sim, da do agente provocador, ao referir no seu parágrafo XXI que:

> O agente provocador convence outrem ao crime, determina a sua vontade para o ato ilícito. O agente infiltrado opera no sentido de ganhar a confiança do suspeito e, na base dessa confiança, mantém-se a par do comportamento daquele, praticando, se necessário, atos de execução em integração no seu plano, mas não assume o papel de instigador. Deste modo, como traço distintivo apresenta-se a passividade do agente infiltrado ou encoberto, o que contrasta com a iniciativa criminosa do agente provocador.

A doutrina e a jurisprudência são mais consensuais na distinção entre as figuras do agente encoberto e do provocador, no entanto, à parte disso, abordar esta destrinça é também fundamental para a compreensão do presente estudo. Para iniciar, salientamos a referência à figura do agente provocador feita por Correia (2016), ao denominá-lo como "aquele que provoca outrem a executar uma atividade criminosa, não porque a queria, mas porque pretende arrastar aquele que determina para a punição" (p. 253).

Silva (1994) diz-nos que a atividade do primeiro passa por apenas informar, não participando no crime, mas que ao invés disso, o provocador "cria o próprio crime e o próprio criminoso" (2005, p.76), reforçando a caracterização da conduta como inaceitável enquanto método de investigação criminal. Gaspar (2004, p. 46) acrescenta mesmo que o crime "não

seria cometido sem a sua intervenção, movido pelo desejo de obter provas da prática desse crime".

No mesmo sentido, Nogueira (1998) entende que o agente provocador dirige a sua atividade de forma a induzir o suspeito à prática de atos ilícitos pelos quais possa ser incriminado, e Meireis (1999, p. 155), advoga que esta figura corresponde àquele que "convence outrem à prática de um crime, (...) pretendendo submeter esse outrem a um processo penal e, em último caso, a uma pena". Para Pereira (1996, p. 48), "enquanto o agente encoberto se limita a observar a prática de crimes (ou pelo menos não os determina), o agente provocador funciona verdadeiramente como instigador desses crimes".

Albuquerque (2011) continua nesta senda, ao dizer que a prova que é obtida em sede de investigação através deste recurso, face ao *modus operandi* em que sucede, será considerada "proibida" (p. 659), uma vez que ofende direitos, liberdades e garantias consagrados constitucionalmente, e recaindo por isso no plasmado no Art.º 126.º n.º 2 al. a) do CPP, ou seja, nos métodos proibidos de prova.

A jurisprudência também tem fluído neste sentido de considerar a atuação do agente provocador e a prova por si recolhida proibidos, tal como no Ac. do STJ n.º 02P4510, de 20 de fevereiro de 2003. O Ac. do TRP n.º 8292/12.6TDPRT.P1, de 7 de maio de 2014, conclui mesmo no seu parágrafo VI que "o agente provocador é agente do próprio crime".

Pereira (2004) esclarece que o Art.º 6.º n.º 1 do RJAE exclui liminarmente a admissibilidade do agente provocador no âmbito das ações encobertas no ordenamento jurídico português[3], uma vez que, segundo o preceituado neste artigo, as condutas atinentes à provocação não granjeiam de qualquer tipo de isenção da responsabilidade criminal para com o agente.

Posto isto, analisaremos agora a figura do terceiro. Desta feita a problemática não se cinge à análise concetual, mas à apreciação de quem poderá assumir esta função no âmbito das ações encobertas. Surge desta circunstância uma nova dicotomia, desta feita entre a figura do terceiro com uma outra, a do informador, cuja diferença é ténue.

Partindo da letra da lei, o RJAE, no seu Art.º 1.º n.º 1, prevê o recurso à figura do terceiro com ocultação da verdadeira identidade para fins de prevenção e repressão da

[3] Para evidenciar o exposto, salientamos sumariamente e a título de exemplo, uma investigação conjunta entre a PJ e a *Drug Enforcement Administration* dos EUA, denominada por «Operação Quimera», que respeita a ações encobertas numa rede de tráfico de droga. Esta fazia transportes desde a Colômbia para Portugal, no entanto, em sede de julgamento, os defensores dos alegados traficantes acusaram agentes destas polícias de terem sido estes a tratarem de toda a logística do transporte do produto estupefaciente aquando das detenções, o que a confirmar-se, se consubstancia na provocação (Vilela & Pinto, 2022).

criminalidade, desde que atuando sob o controlo da PJ e de acordo com o requisito da necessidade de autorização da AJ[4] competente, respetivamente do MP ou do Juiz de Instrução Criminal (JIC) (n.ºs 3 e 4 do Art.º 3.º).

Desta definição que a lei nos dá podemos aferir que, desde que o terceiro efetue as ações encobertas sob o controlo da PJ e de acordo com os requisitos formais previamente estabelecidos, este pode ser um funcionário de outra polícia, por força do dever de cooperação entre os OPC[5]´s, determinado no Art.º 10.º n.º 1 da Lei n.º 49/2008, de 27 de agosto, ou seja, da lei da organização da investigação criminal (LOIC).

No entanto, para Ramos (2022, p. 60) "um terceiro que revele à polícia prática iminente de um crime ou de quem foram os seus autores não atua (...) na qualidade de agente encoberto", devido à inexistência dos formalismos necessários. A jurisprudência também segue esta linha, e.g. o Ac. do TRP n.º 2039/14.0JAPRT.P1, de 7 de julho de 2016, que refere o seguinte:

> É denunciante ou informador e não agente encoberto a pessoa que tem conhecimento que alguém planeia a prática de um crime e disso informa a polícia. Integra-se nessa categoria o agente que tendo sido contactado pelo arguido para facilitar ou colaborar na prática de um crime planeado, o denuncia à autoridade policial, a qual, a partir daí vigia o desenrolar dos acontecimentos com vista à detenção do autor do crime.

No que concerne à lei, não é líquido que o terceiro tenha de ser obrigatoriamente um OPC ou que possa ser um particular. Relativamente à hipótese de ser um particular, esta poderia recair eventualmente sobre um informador que fizesse chegar a *notitia criminis* e despoletado a respetiva investigação. Iniciada a mesma assumiria a figura do agente encoberto enquanto terceiro, sob o controlo da PJ, e tentaria obter a prova necessária à incriminação, ainda que não necessitasse da ocultação da verdadeira identidade por já estar de alguma forma envolvido no meio.

Ramalho (2017) defende esta tese, referindo que este civil poderá integrar a investigação, pois conseguirá as informações com recurso aos seus contactos e pelos

[4] Por AJ entende-se Autoridade Judiciária, que de acordo com a al. b) do n.º 1 do CPP, são o juiz, juiz de instrução e o MP, cada um relativamente aos atos processuais que cabem na sua competência.

[5] Por OPC entende-se órgão de polícia criminal, que de acordo o a al. c) do n.º 1 do CPP, são todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer atos ordenados por AJ ou determinados pelo próprio Código.

conhecimentos específicos. Acrescenta ainda que "revela-se particularmente difícil ou mesmo inviável a infiltração de um agente da polícia num meio criminoso ou a mera interação com o suspeito de modo a que este forneça elementos probatórios" (p. 298).

Já para Costa (2014), é de alto risco o desempenho desta figura por pessoa ocasional que não tenha vínculo de fidelidade ao estado, estatuto inerente aos OPC´s. Valente (2019) acrescenta que o desempenho desta figura mesmo por polícias "levanta alguns problemas no que se refere à restrição de direitos, liberdades e garantias" (p. 418), pelo que sendo feito por particulares ainda mais, uma vez que pode envolver interesses pessoais quanto à investigação, dando-lhes vantagem perante as operações da polícia. Catana (2018) salienta a diferença entre esta figura ser desempenhada por particulares vulneráveis ou profissionais treinados, destacando que, mesmo assim, os segundos não podem ser garantia de sucesso devido a uma hipotética exposição à angariação de dividendos em proveito próprio.

Noutros ordenamentos jurídicos, países como Espanha, França, Alemanha, Argentina e Brasil não permitem o recurso a terceiro que não sejam polícias (Castro, 2012). De acordo com Santos (2020), há ainda países que permitem este tipo de ações encobertas por particulares, aos quais são reconhecidas especificidades em que tenham uma relação com os investigados, pelo que estes tipos de ações são autónomas. Deu (2019) dá o exemplo da Colômbia, paradigma em que, havendo essa relação de confiança entre o particular e o investigado, não necessita sequer de mudar a identidade e os atos limitar-se-ão à obtenção de informações relevantes e elementos materiais probatórios (as cited in Santos, 2020).

Posto isto, e com a devida reverência, inclinamo-nos para a doutrina que aceita apenas os OPC's e recusa a utilização de particulares enquanto terceiros em ações encobertas. Concordamos também com o recurso a particulares civis apenas enquanto informadores, tal como para autores como Andrade (2009a) e Sousa (2010).

Jaramillo (2010) completa esta corrente afirmando que a figura dos informadores se deve cingir a indivíduos de determinados meios delinquentes, que por alguma razão ganham a confiança de polícias, aos quais reportam informações relevantes para a investigação criminal. Castro (2012) acrescenta que, noutro sentido, ordenamentos jurídicos como o francês e o alemão, permitem mecanismos de negociação que incluem mesmo o recurso a pagamentos. É de salientar que, ainda assim, o OPC não deve a qualquer momento indicar a fonte da informação, de modo a não colocar o informador em situação de vir a sofrer represálias, uma vez que este será próximo das pessoas que denuncia (Ramos, 2022). A informação deve ser alvo de técnicas de investigação criminal que possam confirmar a sua veracidade e consubstanciar meios de prova (Fernandes, 2014).

No tocante a esta matéria acrescentamos que a Lei n.º 9/2007, de 19 de fevereiro, a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa (SIRP), do Serviço de Informações de Segurança (SIS) e do Serviço de Informações da República Portuguesa (SIED), veio prever no seu Art.º 12.º o recurso a ações encobertas, ainda que não utilize este termo, por parte dos seus funcionários operacionais para efeitos de recolha de informações. Segundo este, podem ser codificadas as respetivas identidade e categoria, através da emissão de documentos legais de identidade alternativa, aplicando-se o mesmo, com as necessárias adaptações, aos meios materiais e equipamentos utilizados.

As informações recolhidas neste âmbito não podem servir de meio de prova em sede de investigação criminal e os agentes não beneficiam da impunidade prevista no Art.º 6.º n.º 1 do RJAE, no entanto, eventuais indícios da prática de crimes podem e devem ser transmitidos às autoridades competentes (Pereira, 2004).

Como pudemos verificar, as fronteiras que delimitam estas figuras são por vezes muito ténues. Enquanto as figuras do agente encoberto e infiltrado se colocam maioritariamente no plano doutrinal, a destrinça entre estes e o agente provocador, ou da figura do terceiro para com a do informador, já podem colocar, se não forem salvaguardados determinados expedientes, o estado a violar direitos, liberdades e garantias constitucionais.

1.3. Regime jurídico do agente encoberto

Depois de tecidas as considerações sobre a evolução histórica da figura do agente encoberto e da delimitação concetual para outras figuras, nomeadamente do agente infiltrado, do agente provocador e do terceiro, é agora o momento de versar concretamente o regime jurídico do agente encoberto, pois como ensinado por Ferreira (2010), a validade formal respeita à existência da norma.

É no RJAE que se disciplinam as ações encobertas para fins de prevenção e investigação criminal em termos gerais. Para Matos (2015), este regime deveu-se a uma especial dificuldade na investigação e obtenção de provas em determinados crimes, pelo que foi necessário acrescentar tal método na ordem jurídica portuguesa.

Ao apresentar o Projeto de Lei n.º 79/VIII, relativo ao RJAE, António Costa[6] defendeu a introdução desta lei com a necessidade de combater a "globalização da criminalidade transnacional", respondendo, por isso, com a "globalização da repressão da

[6] Ministro da Justiça do XIV Governo Constitucional.

criminalidade". Acrescentou ainda no seu discurso[7] a tónica de que "uma maior eficácia no combate à criminalidade significa maior segurança para os cidadãos", eficácia essa que, segundo o mesmo, seria essencial melhorar na prevenção do crime grave e organizado e na recolha de prova que assegure a efetiva condenação dos criminosos, e na prevenção e repressão da violência criminal.

O RJAE começa por definir no seu Art.º 1.º n.º 2 o conceito de ações encobertas, determinando como tal as que forem "desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da [PJ] para prevenção ou repressão dos crimes" abrangidos, "com ocultação da sua qualidade e identidade".

Com a entrada em vigor deste diploma foram revogados os Art.ºs 59.º e 59.º-A da Lei n.º 15/93, de 22 de janeiro[8] e o Art.º 6.º da Lei n.º 36/94, de 29 de setembro. Desta feita, perdeu-se a exclusividade de recurso às ações encobertas na investigação criminal dos crimes relativos ao tráfico ilegal de estupefacientes e ao combate à criminalidade económico-financeira, abrindo um novo espetro de crimes. Pereira (2004) acrescenta que ainda assim, era de notar que nas posteriores revisões do CPP, o legislador ainda não tinha optado por incluir este recurso nos meios de obtenção de prova. Atualmente, tal desiderato ainda não sucedeu, pelo que são considerados enquanto meios de obtenção de prova no CPP os exames, as revistas e buscas, as apreensões e as escutas telefónicas, cfr. Art.ºs 171.º e ss do mesmo diploma.

Os crimes que contemplam o recurso às ações encobertas são os elencados no Art.º 2.º do RJAE, a saber, (a) o homicídio voluntário, desde que o agente não seja conhecido; (b) contra a liberdade e contra a autodeterminação sexual a que corresponda, em abstrato, pena superior a 5 anos de prisão, desde que o agente não seja conhecido ou sempre que sejam expressamente referidos ofendidos menores de 16 anos ou outros incapazes; (c) relativos ao tráfico e viciação de veículos furtados ou roubados; (d) escravidão, sequestro e rapto ou tomada de reféns; (e) tráfico de pessoas; (f) infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo; (g) captura ou atentado à segurança de transporte por ar, água, caminho-de-ferro ou rodovia a que corresponda, em abstrato, pena igual ou superior a 8 anos de prisão; (h) executados com bombas, granadas, matérias ou engenhos explosivos, armas de fogo e objetos armadilhados, armas nucleares, químicas ou radioativas; (i) roubo em instituições de

[7] Cfr. reunião plenária de 21 de junho de 2001, publicada no Diário da Assembleia da República n.º 99/2001, I Série (p. 16).
[8] Neste diploma legal utilizava-se o termo «infiltrado» ao invés de «encoberto».

crédito, repartições da Fazenda Pública e correios; (j) associações criminosas; (l) relativos ao tráfico de estupefacientes e de substâncias psicotrópicas; (m) branqueamento de capitais, outros bens ou produtos; (n) corrupção, peculato e participação económica em negócio e tráfico de influências; (o) fraude na obtenção ou desvio de subsídio ou subvenção; (p) infracções económico-financeiras cometidas de forma organizada ou com recurso à tecnologia informática; (q) infracções económico-financeiras de dimensão internacional ou transnacional; (r) contrafação de moeda, títulos de créditos, valores selados, selos e outros valores equiparados ou a respetiva passagem; e, por fim, (s) relativos ao mercado de valores mobiliários.

No tocante ao alargamento do espectro de crimes de âmbito de aplicação das ações encobertas, Pereira (2004) refere que este novo catálogo tem "uma composição variada em que coexistem preocupações político-criminais distintas: gravidade do crime (homicídio); dificuldades de prova (crimes sexuais): combate à criminalidade organizada e violenta; tutela de bens jurídicos estatais e sociais" (p. 19).

Já sabemos que mais tarde a LCiber, no seu Art.º 19.º, trouxe também a admissibilidade do recurso às ações encobertas na investigação criminal relativa aos crimes previstos na mesma e aos cometidos por meio de sistema informático, quando respeitarem determinados requisitos[9].

Para além dos crimes inventariados nestes diplomas é ainda de ressaltar a referência às ações encobertas na alteração que a Lei n.º 104/2001, de 25 de agosto efetuou à Lei n.º 144/99, de 31 de agosto, que aprova a lei de cooperação internacional em matéria penal. Neste seguimento aditou-lhe o Art.º 160.º-B, que passou a admitir a funcionários de investigação criminal de outros estados que desenvolvessem essas ações em Portugal, com o mesmo estatuto dos funcionários de investigação criminal portugueses, necessitando para isto da autorização de um juiz do Tribunal Central de Investigação Criminal (TCIC), sob proposta do magistrado do MP junto do Departamento Central de Investigação e Acão Penal (DCIAP), cfr. n.º 3 do mesmo Art.º.

Ainda relativamente a esta matéria, salientamos a Lei n.º 88/2017, de 21 de agosto[10], cujo Art.º 41.º prevê que por meio de deste mecanismo da UE, se possa solicitar a realização de ações encobertas para fins de investigação criminal noutros estados membros.

[9] No que diz respeito à figura do agente encoberto em ambiente digital que surgiu neste âmbito e ao catálogo de crimes em que é admissível, vd cap. II.

[10] Regime jurídico da emissão, transmissão, reconhecimento e execução de decisões europeias de investigação em matéria penal, que transpôs a Diretiva 2014/41/EU, do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal.

Por fim, há ainda referência às ações encobertas na Lei n.º 23/2007, de 4 de julho, que respeita ao regime jurídico de entrada, permanência, saída e afastamento de estrangeiros do território nacional. A mesma institui que as ações encobertas são efetuadas pelo Serviço de Estrangeiros e Fronteiras (SEF)[11] de acordo com o regime geral no âmbito da prevenção e investigação de crimes relacionados com a imigração ilegal, *ex vi* do Art.º 188.º n.º 2.

Retomando o estudo do RJAE, os requisitos que o legislador consagrou para se poder fazer recurso às ações encobertas são os previstos no Art.º 3.º, sendo que o n.º 1 preceitua que estas só são admitidas quando se revelem adequadas e proporcionais às finalidades de prevenção e repressão e, também, à gravidade dos crimes sob investigação. Para Pereira (2004), relativamente ao primeiro requisito pode-se reconhecer uma alusão implícita ao princípio na necessidade, já quanto ao segundo, está efetivamente patente uma exigência de proporcionalidade *stricto sensu*.

Ramos (2022) diz-nos que com este artigo o legislador dá as traves mestras que balizam a utilização deste recurso, invocando "os corolários constitucionais da necessidade, adequação e proporcionalidade" (p. 37), fixados no Art.º 18.º n.º 2 da Constituição da República Portuguesa (CRP), impondo "limites concretos para a sua utilização concatenando os mesmos com os princípios constitucionais a que qualquer *infra lege* deve obediência" (p. 37).

Os n.ºs 3, 4 e 5 do Art.º 3.º estabelecem que é sempre necessária autorização da AJ competente para se fazer recurso às ações encobertas. No âmbito da investigação criminal autoriza o magistrado do MP, *dominus* do inquérito, que deve comunicá-la ao JIC para validação, considerando-se como tal, se não for proferido despacho de recusa no prazo de 72h. O MP é a entidade competente e permanece com o processo, sem qualquer necessidade de comunicação adicional ao JIC. Relativamente ao âmbito da prevenção criminal, autoriza o JIC, mediante proposta do magistrado do MP.

Chamamos à colação os Art.ºs 32.º n.º 4 e 202.º n.º 2 da CRP, segundo os quais cabe ao JIC analisar objetivamente quais os bens jurídicos em conflito e se no caso concreto há restrição dos direitos fundamentais que justifique o recurso à ação encoberta. Segundo Andrade (2009a), o juiz autoriza o recurso às ações encobertas, total ou parcialmente, ou indefere-o. Uma vez autorizado, deve fundamentar os motivos que levaram a tal decisão,

[11] No momento do *terminus* desta investigação, o SEF está a ser alvo de uma remodelação, *ex vi* da Lei n.º 73/2021, de 12 de novembro, que aprova a reestruturação do sistema português de controlo de fronteiras, procedendo à reformulação do regime das forças e serviços que exercem a atividade de segurança interna e fixando outras regras de reafectação de competências e recursos deste serviço. De acordo com a al. c) do n.º 2 deste diploma, as ações encobertas efetuadas pelo SEF passarão para o âmbito da PJ.

delimitar temporalmente e definir os moldes da ação, as pessoas visadas e os meios a serem utilizados. Albuquerque (2011) acrescenta que, por constituírem uma restrição aos direitos fundamentais particularmente intensa, o recurso a este tipo de ações se insere no princípio da reserva de juiz. Valente (2019) defende que a AJ competente deveria ser sempre o JIC, pois uma operação destas "impõe uma preparação tática, técnica, ética e jurídica" (p. 614), que afasta desde logo o *periculum in mora*.

Sublinhamos que, de acordo com o Art.º 3.º n.º 2, "ninguém pode ser obrigado a participar numa ação encoberta", seja qual for a sua qualidade. António Costa, na apresentação do Projeto de Lei n.º 79/VIII, relativo ao RJAE, salientou o quão sensível se pode tornar a segurança dos agentes que efetuem ações encobertas, tanto por conviverem junto a criminosos como por eventuais represálias futuras que daí advenham, pelo que nas normas de proteção dos agentes se prevê a formalização de identidade fictícia, o que foi uma das novidades desta lei.

A identidade fictícia prevista no Art.º 5.º, com a mesma epígrafe, "é atribuída por despacho do Ministro da Justiça, mediante proposta do Diretor Nacional da PJ", sendo que o despacho é classificado como secreto e tem de incluir a referência à verdadeira identidade do agente que desempenha a ação encoberta. A identidade atribuída é válida pelo período de 6 meses prorrogáveis por iguais períodos, ficando o agente autorizado a atuar sob a mesma quer no exercício das suas funções quer em todas as circunstâncias de foro pessoal do seu quotidiano.

Ainda por razões de proteção para com o agente que efetuou a ação encoberta, a AJ só ordenará a junção do processo do relato se este for absolutamente necessário enquanto meio de prova, *ex vi* do Art.º 4.º n.º 1.

Outras medidas de proteção que assistem ao agente que efetuou a ação encoberta são os elencados no Art.º 4.º, nomeadamente a possibilidade de aquele que atuou sob identidade fictícia, oficiosamente ou a requerimento da PJ, prestar depoimento sob a mesma identidade em processo relativo aos fatos objeto da sua acusação, mediante decisão fundamentada da AJ competente.

No caso de o juiz determinar que é indispensável a comparência em sede de julgamento do agente encoberto, este poderá dispor do previsto no Art.º 87.º n.º 1 do CPP, nomeadamente a possibilidade de o juiz decidir, por despacho, oficiosamente ou após requerimento do MP ou do arguido, de restringir a livre assistência do público ao ato, ou a parte dele. Ao agente são ainda conferidos os direitos da Lei n.º 93/99, de 14 de julho, que regula a aplicação de medidas para proteção de testemunhas.

É possível que durante a sua atuação de caráter encoberto, de modo a não criar desconfiança no(s) investigado(s) e, portanto, por razões da própria segurança, o agente tenha de praticar determinados atos que possam incorrer em ilícitos criminais, pelo que o legislador salvaguardou uma cláusula de isenção da responsabilidade. Assim, estabelece o Art.º 6.º n.º 1, que o agente encoberto, no âmbito da sua atuação, pode praticar atos preparatórios e de execução desde que tal não consubstancie autoria mediata ou instigação.

Para Pereira (2004, p. 24), a "conduta do agente encoberto seria justificada por uma causa de exclusão da ilicitude estritamente penal", resultando daqui três cenários, a saber, (a) que o estado pode ser responsabilizado por prejuízos causados a inocentes durante a ação encoberta, (b) que só o agente encoberto, mas não outros comparticipantes no crime, está isento desta responsabilidade penal, e ainda, (c) que está também isenta de responsabilidade a reação de pessoas inocentes que sejam vítimas de agressões, ao abrigo da legítima defesa.

Após o *terminus* da intervenção do agente encoberto, a PJ tem 48 para enviar o relatório da mesma à AJ, de acordo com o n.º 6 do Art.º 3.º.

Chegada a fase do julgamento em processos nos quais houve recurso a prova obtida pela figura do agente encoberto, constata-se que por vezes o juiz não sabe de antemão a proveniência dessa prova. Esse conhecimento antecipado sucede quando o JIC manda juntar ao processo as informações relativas ao exercício da ação encoberta, pois caso contrário, a lei não prevê a obrigatoriedade de tal informação.

Para terminar este périplo à Lei n.º 101/2001, de 25 de agosto, salientamos que esta teve até ao momento três alterações à sua redação inicial. A primeira foi o acréscimo do crime de "tráfico de pessoas" ao catálogo do Art.º 2.º, *ex vi* da Lei n.º 60/2013, de 23 de agosto, que transpôs para a ordem jurídica interna a Diretiva n.º 2011/36/UE, do Parlamento Europeu e do Conselho, de 5 de abril, relativa à prevenção e luta contra o tráfico de seres humanos e à proteção das vítimas.

A segunda foi a introdução na sua redação de "organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo" no catálogo de crimes do Art.º 2.º, *ex vi* da Lei n.º 61/2015, de 24 de junho, que permitiu na sua inclusão todos os ilícitos criminais relacionados com o terrorismo.

A terceira e última foi a alteração da redação da al. f) do Art.º 2.º para "infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo", *ex vi* da Lei n.º 2/2023, de 16 de janeiro, que transpôs para o ordenamento jurídico português a Diretiva (UE) 2017/541, de 15 de março de 2017, relativa à luta contra o terrorismo.

1.4. Breves apreciações sobre as especificidades técnico-práticas

No subcapítulo anterior abordamos a proteção que o legislador proporciona perante os riscos e perigos em que as ações encobertas podem colocar os agentes, nomeadamente a possibilidade da atribuição de identidade fictícia e, em caso de imperatividade da sua presença em sede de julgamento, garantia de proteção da verdadeira identidade.

Destarte, é evidente, para além do fato de atuar sob uma identidade que não a verdadeira, que as ações encobertas se revestem para o agente de especificidades técnico-práticas muito próprias. É necessário que este tenha atributos éticos e morais, entre outros, de modo a não ferirem os direitos, liberdades e garantias dos investigados, prerrogativa de qualquer atividade em representação dum estado de direito democrático.

Naquilo que diz respeito às ações encobertas ditas tradicionais, e antes de avançarmos para o paradigma do agente encoberto em ambiente digital, fazemos menção a algumas dessas especificidades, de modo a melhor compreendermos as razões que levaram o legislador a criar tais mecanismos legais de proteção. Neste subcapítulo temos também a intenção de dar um pequeno contributo relativamente àquelas que são as características das ações encobertas e de toda a sua complexidade técnico-prática, para além da parte estritamente legal.

No que concerne ao recrutamento, Ferreira (1996) refere que este deve ser um processo rigoroso, para além da posterior formação e supervisão das ações encobertas, tendo em vista evitar o fracasso das operações. Acrescenta ainda a mesma autora que estes agentes devem ser treinados ao nível prático em técnicas de representação, linguagem, hábitos e outros aspetos da comunidade em que vão atuar, para além de formação teórica, onde se inclui o direito penal, processual penal e criminalística, entre outros saberes.

Pereira F. (2016) afirma que se deve procurar o perfil certo para cada ambiente em que ocorra a ação encoberta, tendo-se para isso em conta as características da missão, tais como o "tamanho, complexidade, local da atuação", elencadas por Zanella (2016, p. 234).

Regressando ao fator da atuação sob identidade fictícia, vimos que o legislador anuiu aos riscos que uma missão com estas características oferece, respondendo perante os mesmos com as medidas de proteção previstas no Art.º 4.º do mesmo diploma. Dessas medidas elencadas evidenciamos a do n.º 4, na qual o legislador impõe a aplicação do regime de proteção de testemunhas em processo penal ao agente encoberto[12]. Já neste, no seu Art.º 4.º n.º 1, o legislador permite que o agente que usou da identidade fictícia preste declarações ou

[12] Cfr. Lei n.º 93/1999, de 14 de julho.

depoimento com "ocultação da imagem ou distorção da voz, ou de ambas, de modo a evitar-se o reconhecimento".

Os agentes que desempenhem ações encobertas estão eventualmente sujeitos durante as mesmas a uma pressão constante. Ainda que estes sejam previamente preparados e treinados para tal, autores como Oneto (2005) e Ferreira (1996), defendem a tese dos agentes terem de possuir particulares capacidades, devido à dificuldade inerente à gestão das mentiras que hipoteticamente vão ter de construir ao longo do tempo, principalmente quando as operações são por períodos longos, de modo a salvaguardarem a coerência da nova personagem e a sua própria segurança.

De acordo com Ferreira (1996), a própria troca de identidades causa *per si* destabilizações que podem causar stress e angústia. Acrescenta que nos relatos das suas intervenções, os agentes referem muitas vezes o estado de ansiedade, tensão devido ao perigo, e confusão com o próprio nome, concluindo que "quanto maior a pressão, mais (...) procuram fugir às exigências legais para atingirem o resultado pretendido" (p. 568), podendo colocar em causa a sua segurança, a legalidade da sua atuação e concomitantemente levar à nulidade da prova obtida.

Neste mesmo sentido vai a jurisprudência, crf. Ac. do TC n.º 578/98, de 14 de outubro de 1998, o qual refere que:

> A verdade material não pode conseguir-se a qualquer preço: há limites decorrentes do dever de respeito pela integridade moral e física das pessoas; há limites impostos pela inviolabilidade da vida privada, do domicílio, da correspondência e das telecomunicações, que só nas condições previstas na lei podem ser transpostos. (...)
>
> Se o funcionário de investigação criminal encarregado dessa missão não for pessoa de sólida formação moral e firmeza de carácter, pode facilmente deixar-se envolver nas atividades criminosas que investiga.

Capítulo II. As ações encobertas em ambiente digital

2.1. Advento da cibercriminalidade

Estudamos no capítulo anterior todos os aspetos que consideramos importantes para compreender as ações encobertas tradicionais, ou seja, em ambiente físico. Prosseguimos agora com um introito à evolução tecnológica que trouxe consigo o advento da cibercriminalidade, fenómeno sobejamente utilizado hodiernamente, e que levou a que surgissem as ações encobertas também no âmbito digital.

A sociedade atual assenta num paradigma, que, como referido por Bauman (2005), é líquida e tem propriedades voláteis, que a tornam imprevisível, flácida, espontânea, e que traz, desta feita, novos riscos associados.

De acordo com Braz (2020), vários autores chegam a intitulá-la por sociedade de risco, sendo que Beck (1998), apresentou mesmo um modelo pelo qual concluiu que, hodiernamente, existe muito maior capacidade humana para produzir riscos a si mesma do que os próprios riscos de ordem natural. Outro desses autores é Dias (2001), que a descreve como sendo "exasperadamente tecnológica, massificada e global, onde a ação humana (...) se revela suscetível de produzir riscos também eles globais ou com tendência para tal, suscetíveis de serem produzidos em tempo e em lugar largamente distanciado da ação que os originou ou para eles contribuiu" (p. 158).

Esta incerteza e imprevisibilidade têm vindo a ser acompanhadas nas últimas décadas pela evolução das tecnologias da informação. Enquanto nos anos 80 e 90 do século passado a internet era ainda limitada a um nicho muito restrito de utilizadores e em contextos muito específicos, atualmente isso já não acontece, estando facilmente disponível para todos, e na qual é possível fazer quase tudo a partir de um computador, *tablet* ou *smartphone*, e de qualquer localização. Segundo Mata (2011), a internet transformou-se mesmo numa das melhores invenções da humanidade para a maior parte das pessoas, tratando-se de uma "revolução tecnológica que chega a todos os âmbitos culturais, sociais, económicos, e inclusivamente, ao setor judicial" (p. 1).

Existe uma nova organização coletiva proveniente da utilização exacerbada das tecnologias da informação, que resulta de uma rutura tecnológica, social e económica com o período anterior, cujo impacto na história pode ser comparável àquele que teve a revolução industrial (Castells, 2005).

De acordo com Murray (1997), estas novas possibilidades tecnológicas proporcionam interatividade e hipóteses quase que infinitas de exploração, pesquisa e

navegabilidade entre e pelos seus utilizadores. É possível quase todo o tipo de transações comerciais e bancárias, comunicações e outras prestações de serviços, sem necessidade de deslocação e com custo reduzido

Estas novas tecnologias, com a internet como figura de proa, são um bem necessário e útil, no entanto, trouxeram consigo a eventualidade do reverso da medalha, ou seja, de ser possível retirar também de si partido para fins ilícitos, através de novos *modi operandi* (Ramos, 2022). Segundo Carrapiço (2005), são uma faca de dois gumes, pois podem ser manipuladas no âmbito das atividades ilícitas, mas também podem ser utilizadas para combater estas últimas, e assim sucessivamente.

De acordo com o aprendido com Palma (2017), a sociedade é um sistema com determinados níveis, e aplicado às relações interpessoais, onde todos estes níveis de encadeamento se relacionam entre si, gerando uma grande complexidade de comportamentos que carece de regulação. Para a autora, o direito desempenha essa tarefa e está, por isso, em toda a parte. Acrescenta Dias (2004, p. 59) que "as soluções concretas dos problemas básicos dependem fundamentalmente do estádio de evolução e desenvolvimento social e cultural de uma certa comunidade".

Costa (1998) evidenciou a necessidade de se regularem penalmente as condutas praticadas através da internet, pois, segundo este, "a informação automatizada é uma realidade tão essencial que se, por hipótese (...) se bloqueasse, totalmente e à escala mundial, o fluxo informacional automatizado, ainda que por breves horas, todos convêm em considerar que o caos se institucionalizaria" (p. 16).

Esta nova tipologia de crimes perpetrados pelos meios informáticos denomina-se comummente por cibercriminalidade, embora encontremos vários outros conceitos na literatura. Desde logo, Venâncio (2011) começa por fazer a separação da criminalidade informática em dois sentidos, respetivamente o amplo e o estrito. Para este autor, a criminalidade informática em sentido amplo é a que "englobará toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento (...), pelo que o mesmo crime poderá ser praticado por recurso a outros meios" (p. 17). Já em sentido estrito define-o como o que "abarcará apenas aqueles crimes em que o elemento digital surge como parte integradora do tipo legal ou mesmo como seu objeto de proteção" (p. 17).

Verdelho (2003, p. 356) faz uma separação tripartida das "realidades sociológicas de tipo criminógeno" relativamente à cibercriminalidade. Para o mesmo, a primeira trata-se dos crimes perpetrados por via de computadores, mas que poderiam acontecer por outra via,

sendo essa a única característica que os distingue. A segunda é relativa a crimes que não poderiam ser cometidos de outra forma, mas apenas neste ambiente informático. À terceira o autor apelida de "crimes informáticos propriamente ditos" (p. 356), e diz respeito, segundo este, aos que se consubstanciam com recurso a computadores[13], no entanto com a particularidade de serem praticados através da internet.

Salientamos a conceção de cibercrime da Comissão das Comunidades Europeias (2007), segundo a qual são "os atos criminosos praticados com recurso a redes de comunicações eletrónicas e sistemas de informação ou contra este tipo de redes e sistemas", à qual acresce ainda "o facto de poderem ser cometidos em grande escala e de ser muito grande a distância geográfica entre o ato criminoso e os seus efeitos" (p. 2).

De acordo com Antunes e Rodrigues (2018, p. 102) "define-se cibercrime como qualquer crime que ocorra no ciberespaço", num leque que inclui "as ações ilícitas praticadas com recurso às redes digitais, nomeadamente a internet", e ainda os crimes "praticados contra sistemas informáticos, os dados e informações alojadas nos sistemas de informação".

Por fim, e também com o intuito de evidenciarmos o aumento da cibercriminalidade no panorama português, fazemos recurso aos relatórios anuais de segurança interna (RASI) dos últimos três anos, respetivamente 2020, 2021 e 2022.

Segundo o RASI relativo ao ano de 2020, houve aumento coincidente com o primeiro estado de emergência, onde podem ter pesado fatores como o "incremento do tempo de utilização do ambiente digital, incluindo o social, o incremento do teletrabalho e a consequente diluição da tradicional segurança perimétrica das organizações ou o incremento do recurso ao comércio eletrónico" (p. 159). Pode ler-se ainda que "o aumento da cibercriminalidade e a exploração do comércio *online* têm vindo a representar oportunidades para os mercados criminais que poderão ter implicações de longo-prazo na sua expansão" (p. 104).

Já o RASI referente a 2021 refere que "no domínio do cibercrime assinalou-se uma trajetória de incremento da ameaça, nomeadamente quando motivada pela crescente profissionalização da cibercriminalidade transnacional altamente organizada e empenhada em atividades extorsionistas ou de fraude digital que incluíram o ciberespaço português entre a sua superfície de ataque" (pp. 32-33).

[13] Por computadores não consideremos apenas o computador para uso individual *stricto sensu*, mas todos os outros aparelhos informáticos que também têm processadores de informação com ligação à internet (e. g. *tablets* e *smartphones*).

Por último, o RASI relativo ao ano de 2022 refere que se verificou "um aumento quer no número, quer na criticidade dos incidentes de cibersegurança registados e analisados", pelo que se "mantém a tendência de crescimento dos últimos anos" (p. 90). Este relatório salienta ainda o novo paradigma geopolítico, nomeadamente a guerra que decorre na Ucrânia, como possível potenciador de novos riscos associados.

Venâncio (2011) refere que facilidades de vária ordem levam a que exista uma clara tendência para o aumento dos crimes *online*, apelidando o fenómeno como "deslocação criminosa para a *web*" (p. 15), e concluindo mesmo que a evolução tecnológica leva pessoas a perpetrar crimes por meios informáticos que jamais o fariam por outros meios. Ramalho (2017) complementa esta ideia e acrescenta que embora os crimes até possam ser os mesmos, estes instrumentos informáticos trouxeram uma tríplice vantagem aos criminosos, correspondendo à desterritorialização da prática criminosa, à rapidez de atuação, e ainda à possibilidade de anonimato.

2.2. Delimitação concetual de ambiente digital

Ao abordamos a temática da cibercriminalidade constatamos não haver consenso quanto à concetualização do ambiente ou espaço onde esta tipologia de crimes decorre, havendo mesmo uma mescla de conceitos, pelo que julgamos necessário abordá-los.

Comecemos pelo conceito de ciberespaço, o qual, de acordo com Elias (2018, p. 303) "não encontra significado ou definição objetiva e universalmente aceite". Este conceito foi utilizado pela primeira vez por Gibson (1984), que o caracterizou como sendo o conjunto de dados computacionais que existem na globalidade das redes digitais. De acordo com o Departamento da Defesa dos EUA, no *Dictionary of Militar and Associated Terms*, ciberespaço é designado como um "domínio global dentro do ambiente de informação, que consiste numa rede interdependente de infraestruturas de tecnologia de informação, na qual se incluem a internet, redes de telecomunicações, sistemas de computadores e os inerentes processadores e controladores" (2021, p. 55).

No ordenamento jurídico português, encontramos uma definição para este conceito no Despacho n.º 13692/2013, de 28 de outubro, relativo a uma orientação para a política de ciberdefesa, onde se pode ler que:

> É por natureza um espaço aberto desprovido de fronteiras tangíveis, onde tanto o setor público como o privado, civis e militares, atores nacionais e internacionais interagem em simultâneo e de forma interdependente e interligada. Por essas razões,

> não é um espaço seguro e protegido, sendo vulnerável a ataques cibernéticos, que podem ter como consequência perdas relevantes no plano económico e social ou constituir uma ameaça séria à Defesa Nacional, quer no plano da degradação ou destruição de infraestruturas críticas quer no plano da neutralização ou negação ao acesso a recursos informacionais.

Ao invés do termo ciberespaço, vários autores referem sistematicamente as expressões «digital» ou «digitais» sem as aprofundarem, no entanto, Murray (1997) denominou categoricamente o espaço onde acontece a cibercriminalidade por ambiente digital.

Para Ramalho (2017), o conceito de ambiente digital "não tem, por si só, significado jurídico" (p. 37), no entanto é útil como meio para assinalar e compreender a distinção entre os contextos físico e digital, este último desprovido de materialidade. Acrescenta mesmo que ambiente digital "engloba apenas os dados informáticos que, de algum modo, são criados, processados, armazenados e são identificáveis em sistemas informáticos, de modo a que podem ser acedidos direta ou remotamente" (p. 37). Desta feita, é tudo o que é acessível a um utilizador através da mediação das tecnologias de informação, onde se inclui a internet, uma intranet ou mesmo suportes de armazenamento.

Catana (2018) caracteriza o ciberespaço como sendo o mesmo que ambiente digital, no entanto Ramalho (2017) discorda, "desde logo porque a existência de uma ligação à internet (...) não é pressuposto da sua existência" (p. 38). Assim, de acordo com o segundo, podemos considerar ambiente digital a informação guardada *offline* no *webmail* e numa *cloud*, ou em formato físico, e. g. *pendrive*, *cd* ou *dvd*.

Castells (2005) trouxe à colação a noção de sociedade em rede que, segundo este, é caracterizada por uma sociabilização assente numa dimensão virtual, que só é possível devido e por meio das tecnologias da informação, acrescentando mesmo que as relações humanas são cada vez mais por este meio virtual. Ainda segundo o mesmo autor, esta rede virtual é definida como um combinado de ligações e conexões que são concomitantemente estruturas comunicacionais entre sujeitos.

Destarte, salientamos também este conceito de ambiente virtual, que, de acordo com Castells (2005), diz respeito sobremaneira às denominadas redes sociais. Para Kaplan e Haenlein (2010), as redes sociais definem-se como sendo "um grupo de aplicações *online* baseadas nos fundamentos ideológicos e tecnológicos da internet, e que permitem a criação

e a troca de conteúdo pelo utilizador" (p. 61). No mesmo sentido, Lempert (2006) diz-nos que estas redes sociais em ambiente virtual são interativas e permitem que os utilizadores dialoguem, partilhem qualquer tipo de conteúdo, formando autênticas comunidades virtuais.

Extrapolando a tese defendida por Ramalho (2017) para o nosso objeto de estudo, a qual é complementada por Ramos (2022), deduz-se que se uma ação encoberta decorrer com recurso a drones[14] ou GPS[15], ainda que sem necessidade de internet, estamos a fazer uso dum "modo de atuação do agente encoberto digital" (Ramos, 2022, p. 211). Havendo referência a ações encobertas no denominado ciberespaço ou no ambiente virtual, não caberá espaço para dúvidas de que também se tratam de ações encobertas ditas digitais, na medida em que a necessidade de recurso à internet para a existência destes ambientes, torne imperativa a utilização de determinados meios digitais.

Coabita na literatura esta mescla de conceitos, que abarca o de ciberespaço, o de ambiente digital e o de ambiente virtual. Ainda assim, conforme verificamos, a doutrina é unânime em designar esta figura que realiza as ações encobertas ao abrigo do Art.º 19.º da LCiber, por agente encoberto digital, e as ações por si efetuadas como sendo ações encobertas digitais.

2.3. Evolução legal

É o momento de fazermos um levantamento da evolução legal e respetivo enquadramento, que levaram ao aparecimento desta figura do agente encoberto em ambiente digital, começando desde as instâncias internacionais até ao paradigma português.

Ramalho (2017) refere que se foi verificando ao longo do tempo alguma celeuma por grande parte dos países em aceitar a possibilidade de terceiros, estando noutros locais distintos, acederem ainda assim a dados armazenados em *hardware* confinado às suas fronteiras físicas, ao que apelidou de "ingerência não autorizada em território nacional e uma violação da soberania nacional" (p. 67).

Devido a esta resistência, apenas a Recomendação do Conselho da Europa n.º R(89)9, de 13 de setembro de 1989, trouxe consigo o primeiro vislumbre internacional em matéria de regulação de condutas ilícitas no âmbito da utilização da internet, que, por sua

[14] Drone é o termo utilizado na linguagem comum para designar *Unmanned Aircraift System*, que, de acordo com o Office of the Chairman of the Joint (2021), são aeronaves que não transportam operador humano e que voam com ou sem controlo remoto humano.

[15] GPS é a sigla para *global position system*, tecnologia que permite determinar a posição geográfica dos utilizadores em tempo real (Ramos, 2002).

vez, se materializou no ordenamento jurídico português na Lei n.º 109/91, de 17 de agosto, comumente designada por lei da criminalidade informática.

Esta matéria voltou a ser trazida à discussão no apêndice da Recomendação do Conselho da Europa n.º R(95)13, de 11 de setembro de 1995, sobre os problemas em matéria de processo penal inerentes às tecnologias da informação. Posteriormente, foi criado o Comité Europeu para os Problemas Criminais do Conselho da Europa, formado por um grupo de especialistas em cibercriminalidade, para o qual ficou prevista, segundo Ramalho (2017), a necessidade urgente de se negociarem acordos internacionais que definissem de forma clara a admissibilidade de pesquisas e apreensões internacionais, abordando para atingir tal desiderato questões tanto de trato do direito objetivo como processual.

Em 1997, o Parlamento Europeu emitiu a Resolução sobre a comunicação da Comissão com o título «Conteúdo ilegal e lesivo na internet», atinente à necessidade de identificação por parte de quem publica conteúdo na internet, de modo a poder ser responsabilizado.

A Deliberação CM/DEL/DEC(97)583, de 4 de fevereiro de 1997, criou o Comité de especialistas sobre a criminalidade no ciberespaço, que deu início aos trabalhos que iriam levar a uma versão preliminar do projeto da CCiber. O Conselho da UE emitiu a Posição Comum 1999/364/JAI, de 27 de maio de 1999, acerca das negociações relativas ao projeto, onde se pode ler no seu Art.º 1.º n.º 7 (as cited in Ramalho, 2017, p. 68) que:

> Para efeitos de investigação de uma infração penal grave, que deverá ser definida de forma mais precisa na Convenção, e sob reserva de princípios constitucionais e de salvaguardas específicas para respeitar devidamente a soberania, a segurança, a ordem pública ou outros interesses essenciais de outros estados, poderá ser considerada a possibilidade de uma busca informática transfronteiriça em casos excecionais, nomeadamente em situações de emergência, por exemplo na medida em que tal seja necessário para evitar a destruição ou alteração de provas da infração grave, ou para impedir que seja cometida uma infração suscetível de provocar a morte ou danos corporais graves.

Concluído todo este processo de trabalhos a nível internacional, o Conselho da Europa publicou a CCiber, assinada em Budapeste a 23 de novembro de 2001. Conforme

vimos, surge principalmente devido à necessidade de novos meios de obtenção de prova que incidissem no ambiente digital e à questão do acesso transfronteiriço, pelo que salientamos estes fundamentos logo no seu preâmbulo, nos parágrafos §4, §5 e §6, respetivamente:

> Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional.
>
> Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas.
>
> Preocupados com o risco de que as redes informáticas e a informação eletrónica, sejam igualmente utilizadas para cometer infrações criminais e de que as provas dessas infrações sejam armazenadas e transmitidas através dessas redes.

No que diz respeito à CCiber, esta apresenta uma estrutura tripartida. Correspondem à primeira parte as normas de direito objetivo, ou seja, das condutas ilícitas que os países subscritores devem ter em conta nos seus ordenamentos jurídicos, à segunda parte as normas processuais, e por fim, à terceira parte correspondem as normas atinentes à cooperação judiciária internacional.

Acerca das normas processuais presentes na segunda parte, a CCiber não faz qualquer referência direta à prova obtida por meio das ações encobertas. De acordo com Ramos (2022), os artigos da CCiber mais próximos desta temática do agente encoberto digital são o 20.º e 21.º, uma vez que são referentes à recolha em tempo real de dados relativos ao tráfego e à interceção de dados relativos ao conteúdo, respetivamente.

O Parlamento Europeu publicou a Diretiva n.º 2002/58/CE, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, transposta dois anos volvidos para o ordenamento jurídico português pela Lei n.º 41/2004, de 18 de agosto, cuja versão atualizada corresponde à alteração imposta pela Lei n.º 16/2022, de 16 de agosto.

Posteriormente, foi publicada a Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de fevereiro, respeitante aos ataques contra os sistemas de informações, na qual os principais objetivos foram definir e padronizar conceitos, tipificar condutas enquanto crimes,

e ainda uniformizar as legislações dos estados membros, conforme referido no considerando 7, onde se pode ler que "é necessário completar o trabalho realizado pelas organizações internacionais (...) no domínio da aproximação do direito penal (...) sobre cooperação transnacional no âmbito da criminalidade de alta tecnologia".

O Parlamento Europeu emitiu a Diretiva n.º 2006/24/CE, de 15 de março de 2006, alusiva à conservação de dados nas comunicações eletrónicas, vertida para o panorama português pela Lei n.º 32/2008, de 17 de julho (relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas), sobre a qual nos debruçaremos mais à frente no cap. 3.3.

A Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro, foi substituída pela Diretiva 2013/40/EU, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, no entanto, de acordo com Ramos (2022), os tipos legais "mantiveram-se, nos mesmos moldes" (p. 189), não havendo qualquer mecanismo processual introduzido a salientar.

Terminado este périplo à evolução da legislação internacional em matéria de cibercriminalidade, foquemos agora o nosso estudo na LCiber, que surgiu apenas 8 anos depois da CCiber. Foi em 2009 que Portugal aprovou a CCiber pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro[16], e a ratificou pelo Decreto do Presidente da República n.º 91/2009, de 15 de setembro. A LCiber revogou liminarmente a lei da criminalidade informática que se encontrava em vigor até então.

João Silveira[17], na discussão conjunta da Proposta de Lei n.º 289/X/4.ª, referente à Lei do Cibercrime, salientou que esta atualizava, clarificava e criminalizava condutas relativamente à lei da criminalidade informática, que previa novos meios de preservação de prova adaptados à nova realidade e ainda novas capacidades em matéria de cooperação internacional, o que foi uma das novidades desta lei. A respeito desta, acrescentou ainda no seu discurso[18] que "reforça, assim, o combate ao cibercrime ao mesmo tempo que assegura a proteção dos direitos, liberdades e garantias das pessoas contra este tipo de criminalidade".

Na exposição de motivos da Proposta de Lei n.º 289/X/4.ª pode ler-se que "optou-se por condensar neste diploma todas as normas respeitantes à cibercriminalidade e não por proceder à alteração das várias fontes legislativas sobre a matéria" (as cited in Ramos, 2017,

[16] A ratificação aconteceu ainda que com a reserva prevista no Art.º 2º da Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, relativo ao Art.º 24.º n.º 5 da CCiber, que diz respeito à extradição de pessoas, respeitando-se nesta matéria a ordem jurídica existente.

[17] Secretário de Estado do Ministério da Justiça do XVII Governo Constitucional.

[18] Cfr. Reunião plenária de 9 de julho de 2009, publicada no Diário da Assembleia da República n.º 102/2009, I Série (p. 40).

p. 184) por ser uma opção mais condizente com a tradição portuguesa, nomeadamente na área penal, acrescenta-se.

Analisando de forma sumária tanto a estrutura como aquilo que trouxe de novo, podemos decompor a LCiber em quatro partes. Salientamos desta feita, em primeiro lugar, o correspondente ao cap. I, onde encontramos o objeto e as definições procedentes da CCiber para o ordenamento jurídico português.

Em segundo lugar destacamos, sem o fazermos pela sequência da lei, o atinente à cooperação internacional do cap. IV. Relativamente a este ponto trata-se da criação de ferramentas que solucionem a falta de fronteiras físicas que existem no ciberespaço "para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova"[19].

Como principal produto resultou, *ex vi* do Art.º 21.º, um ponto de contacto permanente para a cooperação internacional, que, de acordo com o seu n.º 1, "assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana" assegurado pela PJ. Este pode ser contactado por outros pontos similares noutros países ao abrigo de "acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais", cfr. o seu n.º 2.

A estrutura aludida foi criada apenas em 2017, dando lugar à terceira alteração à Lei de Segurança Interna[20] (LSI), aditando-lhe o Art.º 23.º-A, com a epígrafe "Ponto Único de Contacto para a Cooperação Internacional" (PUC-CPI). O Dec.-Lei n.º 10/2020, de 11 de março, estabelece a organização e funcionamento deste PUC-CPI, tendo já substituído o Decreto Regulamentar n.º 7/2017, de 7 de agosto.

No que diz respeito às normas de direito objetivo, o legislador acrescentou no cap. II da LCiber, novas condutas puníveis como crimes, mantendo ainda assim os crimes de devassa por meio informático e burla informática nos Art.ºs 193.º e 194.º do Código Penal (CP), respetivamente, optando por não os incorporar nesta lei extravagante.

De acordo com Mesquita (2010), esta lei trouxe ao ordenamento jurídico português ferramentas para a obtenção de prova digital[21], pois antes recorria-se ao estipulado no CPP, o que levava a que a necessidade de obtenção de prova de comunicações efetuadas de forma que não por telefone, gerasse dúvidas.

[19] Cfr. Art.º 20º da LCiber.
[20] Lei n.º 53/2008, de 29 de agosto.
[21] Vd cap. 3.3. para melhor compreender regime da obtenção da prova digital.

A jurisprudência também vai nesse sentido, cfr. parágrafos §1 a §3 do Ac. do TRE n.º 648/14.6 GCFAR-A.E1, de 20 de janeiro de 2015, que refere o seguinte:

> O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às «telecomunicações eletrónicas», «crimes informáticos» e «recolha de prova eletrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.
>
> Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável á recolha de prova por «localização celular conservada» - uma forma de «recolha de prova eletrónica (...)
>
> Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime».

Estas novas normas processuais que Mesquita (2010) refere correspondem ao cap. III da LCiber e são as constantes entre os Art.ºs 12.º e 19.º , a saber, a preservação expedita de dados, a revelação expedita da dados de tráfego, a injunção para apresentação ou concessão do acesso a dados, a pesquisa da dados informáticos, a apreensão de dados informáticos, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, a interceção de comunicações e as ações encobertas, respetivamente.

As disposições processuais citadas aplicam-se, de acordo com o Art.º 11.º, aos processos relativos a crimes previstos na presente lei, cometidos por meio de sistema informático, ou relativamente aos quais seja necessário proceder à recolha de prova em suporte eletrónico, de onde se excetuam a interceção de comunicações e as ações encobertas, justificando-se "pelo carácter bastante intrusivo destas duas diligências" (Catana, 2018, p. 58).

Para terminar este périplo à evolução legal da figura do agente encoberto digital, salientamos que, devido ao aumento da cibercriminalidade, como vimos anteriormente, novas medidas foram sendo tomadas ao longo do tempo. Tal como como referido por Poiares (2019), a sociedade contemporânea tem encontrado no ciberespaço uma plataforma propícia para a reprodução dos seus desvios. Neste sentido, foi aprovada em 2015 uma estratégia

nacional de segurança do ciberespaço[22], cujo objetivo, de acordo com o n.º 1 do seu anexo, consiste no "compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço". Esta estratégia é avaliada e substituída[23] de três em três anos e, no momento do *terminus* desta investigação, está em vigor a publicada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho.

2.4. Regime jurídico do agente encoberto digital

É o Art.º 19.º da LCiber significativo para o nosso objeto de estudo, na medida em que é este que habilita os OPC's, após necessária autorização da AJ competente, a fazerem recurso às ações encobertas em ambiente digital, remetendo a forma para o regime geral previsto no RJAE.

Verificamos que o ordenamento jurídico português não tem um regime específico para regular a atuação do agente encoberto digital, no entanto, de acordo com Ramalho (2017), isto também acontece nos outros ordenamentos que permitem recurso a esta figura, pois em nenhum existe "qualquer previsão legal especificamente direcionada à regulação das ações encobertas em ambiente digital" (p. 283).

O mesmo autor salienta esta "tendência global de não [se] distinguir[em] as ações encobertas em ambiente *físico* das que ocorrem em ambiente digital" (p. 283), com recurso a jurisprudência dos EUA, país onde existe elevado tipo de incidências recorrendo a este meio de obtenção de prova[24], nas duas vertentes. Da decisão do Tribunal do Ohio, relativamente ao caso *United States versus Charbonneau*[25], depreende-se que esta aplicação do regime geral das ações encobertas pode ser extrapolada para o ambiente da internet, (e. g. em salas de *chat* ou nas redes sociais), pois o denominador comum entre ambas é a ocultação da verdadeira identidade com o fim da recolha de prova, o que é concebível.

[22] Cfr. Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho.

[23] Em 2017 foi criado um grupo de projeto denominado por Conselho Superior de Segurança do Ciberespaço, que elabora os anteprojetos que constituem a base à renovação destas estratégias, *ex vi* da Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto.

[24] Salientamos a título de exemplo a investigação que lá deu início e que levou ao desmantelamento de uma rede de pedofilia que operava em fóruns de redes sociais, mas cujo eixo estava sediado na Austrália, onde foram detidos 16 indivíduos (Lusa, 2020).

[25] De forma resumida, este caso respeita a uma investigação perpetrada pelo FBI, na qual um agente efetuou ações encobertas em várias salas de *chat* conotadas com pedo-pornografia. Os utilizadores trocavam este tipo de material pornográfico, e o agente, não participando nas conversações, gravava todo o conteúdo. Por vezes era enviada correspondência com este tipo de material para todos os participantes destes *chats*, a qual o agente também recebia. Um dos participantes que enviava material dessa índole veio a descobrir-se ser Charbonneau. Após buscas à sua residência em Ohio, encontrou-se material pedo-pornográfico, o que levou à respetiva acusação por distribuição de pornografia infantil.

Como já vimos, a sua aparição no ordenamento jurídico português surge pelo Art.º 19.º da LCiber, cuja redação do mesmo é a seguinte:

> 1 - É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:
>
> a) Os previstos na presente lei;
>
> b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos[26].
>
> 2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.

Este método de obtenção de prova surge, de acordo com Ramalho (2013a), devido ao reconhecimento da "necessidade do recurso a métodos de investigação criminal mais agressivos em relação a uma criminalidade que tem beneficiado largamente da ineficácia dos restantes meios disponíveis" (pp. 407-408).

Não obstante, encontramos algumas críticas na doutrina. Com esta norma, o legislador alargou o leque de crimes em que é possível fazer recurso às ações encobertas, para além daqueles já previstos no RJAE. A al. a) do n.º 1 refere-se às condutas ilícitas previstas entre os Art.ºs 3.º e 8.º do diploma, que correspondem aos crimes de falsidade informática, dano relativo a programa ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido. Salientamos que relativamente às infrações económico-financeiras não estamos perante um acrescento, uma vez que estas já estavam previstas no Art.º n.º 2 al. p) do RJAE, disposição

[26] As condutas ilícitas previstas no título IV do Dec.-Lei n.º 63/1985, de 14 de março, são a usurpação, contrafação, violação do direito moral e o aproveitamento de obra contrafeita ou usurpada.

que Dias (as cited in Ramalho, 2017, p. 303) qualifica como "cláusula de insuportável indeterminação".

Valente (2019) considera este catálogo de crimes como sendo heterogéneo, o que "neutraliza os axiomas da subsidiariedade, da excecionalidade e da especialidade do meio de obtenção de prova, dando-lhe uma dimensão de vulgaridade" (p. 620). Autores como Neves (2011), Mesquita (2010) e Ramalho (2017), criticam o fato de o legislador ampliar neste artigo o catálogo de crimes anteriormente previsto no RJAE conjeturando, para isso, uma medida excecional para alguns crimes menos graves, o que lesa os princípios da proporcionalidade e da necessidade, levando o estado eventualmente a perder a superioridade ética, que é sua prerrogativa. Valente (2019) acrescenta mesmo que "o legislador aprovou um regime híbrido que pode gerar conflitualidade normativa e insegurança jurídica" (p. 620), e que este meio de obtenção de prova é um dos "mais ocultos, intrusivos e lesivos dos direitos fundamentais pessoais" (p. 616).

Como verificamos, existe referência no n.º 2 do Art.º 19.º ao recurso a meios e dispositivos informáticos[27], pois de acordo com o estipulado neste, quando for necessário aplicam-se, dentro do possível, as regras previstas para a interceção de comunicações. Assim, segundo Nunes (2021), quando em ações encobertas se utilizarem meios como "*chat*, *website*, *blog* ou fórum de acesso reservado ou conteúdos aí partilhados, haverá que observar o regime do Art.º 18.º" (pp. 437-438).

Ramos (2022) refere que esta remissão para a norma sobre a interceção das comunicações revela como se sai do âmbito das ações encobertas, acrescentando mesmo que para se ter acesso a esses dados não são necessárias estas ações, mas solicitá-los às operadoras de telecomunicações. Assim, "resulta inequivocamente que interceção de comunicações e ações encobertas são figuras distintas de investigação criminal, com catálogos de crimes diferentes e formalidades de operações inigualáveis" (p. 184).

Salientamos que o Art.º 19.º n.º 1 da LCiber prevê o recurso a esta figura "no decurso de inquérito", o que leva Ramos (2022) a afirmar que, desta forma, se "afasta liminarmente que se possa utilizar este regime em ações de prevenção" (p. 183), faculdade existente no RJAE. Sendo assim, quanto aos crimes de catálogo para os quais esta lei prevê o recurso às

[27] A al. a) do Art.º 2.º da LCiber define sistema informático como sendo qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução 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 funcionamento, utilização, proteção e manutenção.

ações encobertas, existe uma ablação de possibilidades, ficando apenas contemplada a faculdade para efeitos de investigação criminal.

Existem também na doutrina várias referências às principais vantagens desta modalidade de ações encobertas, nomeadamente quando feita a comparação com as ações encobertas tradicionais. Autores como Ramos (2017) e Nunes (2021) salientam o fato destas permitirem que a mesma pessoa «real» utilize várias identidades fictícias em simultâneo, ou que a mesma pessoa «fictícia» possa ser operada por diferentes agentes, juntando a isto a particularidade de se poder operar em diferentes locais da *web* simultaneamente. Daqui resulta, de acordo com Ramalho (2017), um "reduzido risco para a segurança do agente" (p. 308), pelo que este "pode falhar, sem que tal implique, em geral, especiais consequências para a sua segurança" (p. 285), ao contrário daquilo que anteriormente pudemos observar para as ações encobertas tradicionais[28].

Relativamente à necessidade de robustez psicológica para se efetuarem ações encobertas digitais, Gómez (2017) diz-nos que, para este tipo de ações poderá existir, embora não de forma igual às de ambiente físico[29], algum tipo de exposição a conteúdo sensível (e. g. o pedo-pornográfico), que eventualmente também pode vir a causar "danos morais" e "problemas psicológicos" (p. 108) ao agente.

[28] Vd cap. 1.4.
[29] Idem.

Capítulo III. A prova obtida pelo agente encoberto em ambiente digital

3.1. A prova enquanto objetivo fundamental da investigação criminal

Agora que iniciamos a nossa abordagem à temática da prova obtida no decurso das ações encobertas digitais, consideramos pertinente começar com um introito relativo ao conceito da prova e à sua relevância na investigação criminal, visto que, segundo Beleza e Pinto (2013, p. 5) "não existe um processo penal válido sem uma prova que o sustente".

De acordo com Ihering (2009, p. 43), tornou-se imperioso que se "regulamentasse a administração da justiça, com normas e uma sequência de atos organizados dentro de um processo, e o mais importante, com a determinação de meios e métodos de resgatar a verdade a bem do justo". Roxin (2000) refere que tal desiderato teve início com a criação de modelos em que os estados passaram a ter limitações no seu poder. Miranda (2014) acrescenta ainda que quando tal matriz de direito processual penal se estabeleceu, deram-se ao acusado direitos enquanto verdadeiro sujeito processual.

Destarte, para Greco (2003), na consciência coletiva dum estado de direito democrático contemporâneo, pode ser considerada como uma ilusão a ampla e eficaz tutela jurisdicional do gozo de todos os direitos dos seus cidadãos. Ainda de acordo com o mesmo autor, "ocorre que o direito nasce dos fatos e não houve até hoje ciência ou saber humano que fosse capaz de empreender uma reconstrução dos fatos absolutamente segura e aceite por todos" (pp. 213-214), de modo a que o juiz se limite a aplicar o direito.

Surge a importância da prova, que tem sido destacada ao longo do tempo por vários autores. Descartes (1989, p. 12) afirmou que, "alicerçados pelas provas, os operadores do direito puderam ajustar as suas bússolas em um norte mais próximo possível da realidade e da justiça". Também Bentham (2001) lhe exprimia tamanha importância, aludindo que "a prova é um instrumento que o processo tomou emprestado da realidade da vida" (p. 15). Giuliani (1971) acrescenta que todo um ordenamento jurídico se reduz a uma ciência das provas e que o próprio direito não existe de forma independente desta, sendo o seu cerne.

O conceito de prova é polissémico, não só na linguagem corrente como também na jurídica. Quanto ao sentido estritamente jurídico, Mendes (2014) estrutura-o em três aceções distintas, a saber, (a) como atividade, ou seja, "destinada a demonstrar a verdade de fatos alegados em juízo - melhor se dirá como atividade probatória" (p. 61), (b) como meio, ou seja, a forma como se vai provar algo, e (c) como resultado, ou seja, "consiste em a verdade

de fatos alegada em juízo ficar demonstrada - esse o sentido mais crucial do termo, em doutrina" (p. 61).

Naquilo que ao ordenamento jurídico português diz respeito, este foi influenciado, de acordo com autores como Albuquerque (2003), Novais (2004) e Dias (2014), pelos legados filosóficos da proteção do indivíduo perante o poder coercivo do estado, e também do aparecimento do estado social e respetiva comunitarização do processo penal. De acordo com Albuquerque (2003), este novo paradigma "judiciário social" (p. 993) ficou assente logo na CRP de 1976.

Portugal é, de acordo com os Art.ºs 2.º e 32.º da CRP, sua *Lex Mater,* um estado de direito democrático com garantias no seu processo penal. O presente modelo relativo a este processo penal é de matriz estruturalmente acusatória agregado por um princípio da investigação[30], pois a entidade que acusa difere da que julga, no qual a prova e a sua produção são fundamentos básicos para se chegar à descoberta da verdade material.

Conforme referido no Art.º 124.º n.º 1 do CPP, "constituem objeto da prova todos os fatos juridicamente relevantes para a existência ou inexistência de crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis". Já no Art.º 341.º do Código Civil (CC), vemos que "as provas têm por função a demonstração da realidade dos factos". Do Art.º 262.º n.º 1 do CPP retiramos que a finalidade e âmbito do inquérito, - ou investigação criminal[31] -, "compreende o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação".

Valente (2019) é mais abrangente, e refere tratar-se do "processo de procura de indícios e de vestígios que indiquem e expliquem e nos façam compreender *quem*, *como*, *quando*, *onde* e *porquê* foi/é cometido o crime *x*" (p. 596). Dias (2016) complementa que a atividade probatória constitui "conditio sine quo non do se e do como da condenação" (p. 5).

Para Silva (2020), a atividade probatória tem como finalidade convencer da existência ou não dos fatos que pressupõem a norma estatuída. Podemos extrair daqui que é o juiz o principal destinatário da prova, na medida em que a esta correspondem os elementos que lhe são levados para o convencer da exatidão dos fatos anteriormente alegados, para que

[30] De acordo com Dias (2014), que complementa não se tratar de um modelo acusatório puro, mas sim misto.
[31] Cuja definição presente no Art.º 1.º da LOIC é similar, referindo ser "o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo".

este forme um juízo de convicção da verdade, e se pronuncie quanto à decisão final. Mendes (2004, p. 132) acrescenta que "a prova consiste no esforço metódico do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medidas de segurança aplicáveis". Neste sentido, Albuquerque (2011) caracteriza a prova como um "facto juridicamente relevante" (p. 329),

No que respeita à admissibilidade e validade da prova, o legislador optou por efetuar uma formulação negativa, ao mencionar que "são admissíveis as provas que não forem proibidas por lei", cfr. o Art.º 125.º do CPP. O regime de proibições de prova delimita aquelas que são as linhas intransponíveis aquando da busca da verdade material sem que tal desiderato colida com a proteção dos direitos fundamentais, sendo as mesmas as estatuídas em dois artigos. O Art.º 32.º da CRP, com a epígrafe "garantias de processo penal", afirma no seu n.º 8 que "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações". O Art.º 126.º do CPP, com a epígrafe "métodos proibidos de prova" refere no seu n.º 1 que "são nulas, não podendo ser utilizadas, as provas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas", e nos seu n.º 3 que, "ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular".

Quanto a estas balizas, Canotilho e Moreira (2007) referem que são uma garantia de intransponibilidade que leva à inutilidade processual em caso de desrespeito, por irem contra a dignidade da pessoa humana prevista no Art.º 1.º da CRP e os princípios que são apanágio do estado de direito democrático, *ex vi* do Art.º 2.º da CRP. Andrade (2009b) salienta ainda que o processo está concebido *prima facie* direcionado para a tutela dos direitos fundamentais, cujo objetivo é tendencialmente o que prevalece, pelo que a prova não pode ser concebida a qualquer custo.

Para concluir esta temática, Gossel (as cited in Andrade, 2013), ensina-nos que as proibições de prova devem ser entendidas como "barreiras colocadas à determinação dos fatos que constituem objeto do processo" (p. 83), ou seja, colocam "de um lado a necessidade de descoberta da verdade material e do outro a proteção dos direitos fundamentais" (Antunes, 2017, p. 16).

3.2. A prova digital e respetivas especificidades

Um dos tipos de prova que existe é a comummente denominada por prova digital. No âmbito do nosso estudo é essencial que se faça uma abordagem a esta temática, uma vez que é tema central a admissibilidade da prova recolhida pelo agente encoberto em ambiente digital, a qual se consubstancia, não raras vezes, respetivamente nesta tipologia de prova.

No cap. 2.2. deste estudo verificamos o emaranhado concetual que existe em torno da temática do ambiente digital no ordenamento jurídico português. O mesmo sucede com a definição de prova digital, na medida em que a mesma nem existe. De acordo com Ramalho (2017, p. 99), o legislador português deixou "espaço para que a jurisprudência e a doutrina preenchessem o vazio". Desta feita, temos de alternar o encaminhamento não para uma definição propriamente dita, mas para a referência à expressão "prova em suporte eletrónico" que é utilizada na LCiber, e para a utilização da expressão "prova guardada em suporte digital" utilizada no CPP.

Neste desiderato que é compreender a pertinência destas e outras expressões quando nos referimos à prova digital, Pradillo (2013) diz-nos que a utilização do conceito de prova digital é encarada com determinada celeuma por parte de alguma doutrina, pelo que o conceito de prova eletrónica acaba mesmo por ser mais consensual. Ramalho (2017) esclarece o conceito de prova eletrónica como sendo mais abrangente, incluindo não apenas a "prova em formato digital, mas também a prova em formato analógico, como sejam as gravações em fita vídeo e áudio ou fotografias em rolo fotográfico, as quais, apesar de digitalizáveis, não têm a sua origem em formato digital" (p. 100).

No que respeita ao conceito de prova digital propriamente dito, Ramos (2022, p. 119) define-o "como sendo toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações". Nunes (2021) pormenoriza-o ainda mais, para o qual se trata da "informação relevante para fins probatórios produzida/obtida a partir de dados em formato digital (...) armazenados, processados ou transmitidos em/através de/entre sistemas informáticos ou armazenados em suportes informáticos, muitas vezes com utilização de redes de comunicações eletrónicas" (p. 47).

Por seu turno, Rodrigues (2009) propõe uma fusão de ambas as conceções anteriores, chamando-lhe prova eletrónico-digital, a qual demarca como sendo "qualquer tipo de informação, com valor probatório, armazenada em repositórios eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas, ou publicamente acessíveis, sob a forma binária ou digital" (p. 722).

Ramalho (2017) esclarece que o termo digital abarca outras tecnologias e sistemas de comunicações que podem não ser eletrónicos, mas que, ainda assim, hodiernamente já se não consegue fazer uma dissociação em termos amplos da informática, pelo que, se "não justifica uma rutura com a terminologia já enraizada na doutrina e jurisprudência" (p. 102).

No que diz respeito à sua tipologia, de acordo com as interpretações de Nunes (2021) e Ramos (2022), a prova digital trata-se de uma forma de prova documental, *ex vi* do Art.º 362.º do CC, que refere denominar-se como documento "qualquer objeto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou fato". Os mesmos autores, ao qual se junta Ramalho (2017), aceitam ainda a possibilidade de se considerar também como um tipo de prova pericial, acrescentando este último que "será necessário recorrer a um especialista em ciência forense digital que, mediante os procedimentos e ferramentas forenses apropriados, poderá, por hipótese, recuperar ficheiros eliminados, encontrar registos da conta utilizada, e, em geral, reconstruir a atividade" (p. 103).

Esta necessidade de cuidados especiais no seu trato, sob pena de "um mero descuido (...) torná-la irremediavelmente inutilizada" (Ramos, 2017, p. 97), é fruto de particularidades intrínsecas. Rodrigues (2011b) afirma que a prova digital tem como características o fato de ser "fragmentária, dispersa, frágil, volátil, alternável, apagável e manipulável, invisível e espacialmente dispersa" (p. 29). A estas, soma-se a variedade e complexidade dos locais de onde pode ser obtida, tais como computadores, (e seus componentes), *tablets*, *smartphones*, dispositivos de armazenamento, câmaras fotográficas e/ou de vídeo digitais, aparelhos periféricos, (como leitores de cartões, impressoras ou *scanners*), gravadores de áudio, sistemas de videovigilância, consolas de videojogos, servidores, *routers*, *access points*, redes de comunicações eletrónicas, entre outros[32].

Nesta senda de especiais particularidades, Antunes e Rodrigues (2018) evidenciam que, considerando a volatilidade do componente de onde se efetua a extração, e de modo a tentar provocar o menor dano possível na prova, deve proceder-se à respetiva extração desde os componentes mais voláteis (e.g. memória RAM) para os menos voláteis (e. g. dispositivos de armazenamento).

Quanto à obtenção deste tipo de prova, Marques (2013, as cited in Ramos, 2022) diferencia-a em dois tipos. A primeira corresponde à prova obtida no próprio local da busca, ou então de modo remoto, sem que os aparelhos sejam retirados desse mesmo local onde se

[32] Cfr. guia de provas eletrónicas do Conselho da Europa (as cited in Ramalho, 2017).

encontram[33]. A segunda corresponde àquela executada *a posteriori*, se necessário em laboratórios especializados para o efeito, após transporte dos aparelhos (Ramos, 2017).

Neste processo continuo da investigação criminal que é a recolha da prova com o objetivo de chegar à verdade material, Palma (2014) destaca três momentos distintos, a saber, (a) a formulação das hipóteses após ampla recolha de informação, (b) o afastamento de hipóteses menos plausíveis e aproximação às mais plausíveis, com recurso também à experiência do investigador e, por fim, (c) a exposição do raciocínio, demonstrando os motivos da conclusão. Fazendo também alusão ao ensinamento da autora para a obtenção da prova, Ramalho (2017) toma como referência, no que diz respeito à obtenção da prova digital em específico, o "modelo quadripartido proposto pelo *National Institute for Standarts and Technology* (NIST)" (pp. 114-115). De acordo com o NIST, as etapas estabelecidas para a obtenção de prova em ambiente digital são a recolha, o exame, a análise e o relatório. Para Ramalho (2017), estas "reúnem os elementos comuns essenciais dos principais modelos e (...) relevam uma maior fluidez procedimental" (p. 115).

Vimos atrás particularidades da prova digital que tornam o acesso a si mais trabalhoso. Agora que abordamos a obtenção deste tipo de prova, chamamos à colação uma outra particularidade salientada por autores como Campos (2021) e Ramos (2022), que é a possibilidade de esta ser previamente encriptada[34]. Assim, mesmo que se tenha acesso à mesma, não raras são as vezes em que não se consegue desencriptar a informação transmitida. Quanto a esta problemática, Ramos (2022) refere que diversas polícias mundiais e o próprio diretor da *European Union Agency for Law Enforcement Cooperation* (Europol) já se manifestaram quanto à necessidade de se encontrarem soluções legislativas para ser possível aceder à informação encriptada por aplicações de comunicações para fins de investigação criminal.

3.3. Regime jurídico da obtenção de prova digital

Na senda da nossa abordagem à prova digital, e procurando desde já começar a responder a um dos objetivos a que inicialmente nos propomos com esta investigação, que é compreender a sistematização da recolha da prova digital no ordenamento jurídico

[33] Fazemos aqui menção à possibilidade do alojamento da mesma informação em locais distintos cujo acesso remoto também pode ser efetuado a partir de vários locais (e. g. *clouds* ou *webmails*), o que, como já vimos anteriormente, trouxe "uma rutura com o paradigma existente até então" (Ramos, 2022, p. 121).

[34] Segundo Marques (2013, as cited in Ramos, 2022, p.156), trata-se de um "método de codificar dados, para transformar texto corrente em texto cifrado, através de uma chave criptográfica de forma a evitar que mais ninguém a não ser o legítimo proprietário leia o seu conteúdo".

português, destacamos agora o referido por Correia (2014), quando rotulou esta regulamentação como um "pântano prático e, sobretudo normativo" (p. 30). Fê-lo porque era então necessário entrosar três diplomas distintos, a saber, o CPP, a LCiber e a Lei n.º 32/2008, de 17 de julho[35].

No que diz respeito ao CPP nesta matéria, a prova digital encontra-se prevista no Art.º 189.º, onde há menção a conversações, comunicações ou dados em "suporte digital". Todavia, esta norma limita-se a fazer a remissão para os Art.ºs 187.º e 188.º do mesmo diploma, que correspondem ao meio de obtenção de prova relativo às escutas telefónicas. Segundo Almeida (2018, p. 46), a "lei penal portuguesa, atribui, em sede de meios de prova, a qualquer conversação ou comunicação transmitida por meio eletrónico diferenciado dos já consagrados na lei (e. g. telefone), a mesma admissibilidade, requisitos e pressupostos das interceções das escutas telefónicas". Acrescenta Correia (2014), que esta norma abrange realidades distintas que careceriam também de tutelas distintas, pelo que o legislador veio desta forma gerar incerteza e insegurança jurídicas.

No que tange à LCiber, importa salientar que esta lei extravagante refere logo no seu Art.º 1.º, que estabelece as disposições penais e processuais penais atinentes à "recolha de prova em suporte eletrónico". Para Almeida (2018, p. 49), este diploma confere "um regime processual penal geral no que respeita à obtenção da prova digital, potencialmente dirigido a todos os tipos de crime". Como já mencionamos anteriormente, os meios de obtenção de prova encontram-se previstos entre os Art.ºs 12.º a 19.º, sendo o último destes o correspondente às ações encobertas digitais.

A jurisprudência, nomeadamente o Ac. do TRE n.º 648/14.6 GCFAR-A.E1, de 20 de janeiro de 2015, explicita esta dinâmica, cfr. podemos verificar nos parágrafos §4 a §7:

> Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos

[35] Veremos adiante neste subcapítulo que no entrosamento referido já não há lugar a este diploma legal.

artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem a Lei 109/2009.

As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte eletrónico.

A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem á pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á interceção de comunicações eletrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático;

Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova eletrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal».

Deixamos para última instância a Lei n.º 32/2008, de 17 de julho, porquanto o Ac. do TC n.º 268/22, de 19 de abril de 2022, declarou padecerem de "inconstitucionalidade, com força obrigatória geral", as normas constantes dos Art.º 4.º (categoria dos dados a conservar), Art.º 6.º (período de conservação), e Art.º 9.º (transmissão dos dados). Isto, por violação dos n.ºs 1 e 4 do Art.º 35.º, n.º 1 do Art.º 26.º, e n.º 1 do Art.º 20.º, em conjugação com o n.º 2 do Art.º 18.º, todos da CRP, ou seja, por violarem o princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar, ao sigilo das comunicações e a uma tutela jurisdicional efetiva.

Esta lei tinha transposto para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente

disponíveis ou de redes públicas de comunicações, que, segundo o mesmo Ac. do TC, já tinha sido declarada inválida pelo Tribunal de Justiça da UE, porque, e sucintamente, "foi entendido que aquela possibilitava uma ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia", ou seja, perante o respeito pela vida privada e familiar e a proteção dos dados pessoais, respetivamente.

Após a declaração de inconstitucionalidade destas normas, concluiu-se na reunião plenária da Assembleia da República de 3 de junho de 2022, que ficou, entre outros, um problema por resolver relativamente à hipótese da geolocalização celular para efeitos de investigação criminal, para o qual Pedro Alves[36] defendeu, como possível solução, que se "harmonize" (p.31) a Lei n.º 41/2004, de 18 de agosto, relativa à proteção de dados pessoais e privacidade nas telecomunicações. Da efetiva alteração ao diploma legal referido, que surgiu *ex vi* da Lei n.º 16/2022, de 16 de agosto, há a salientar que passaram a ser permitidos "o registo, o tratamento e a disponibilização de dados de localização, nomeadamente da informação sobre a localização do chamador, às organizações com competência legal para receber ou tratar comunicações de emergência, para efeitos de resposta a essas comunicações", cfr. Art.º 7.º n.º 2, pelo que aconteceu o referido reforço à possibilidade da geolocalização celular por esta via.

Posto isto, e relativamente ao emaranhado normativo existente em torno desta matéria, Mesquita (2010) e Correia (2014) defendem que, ao criarem-se regimes processuais penais para a prova digital em diplomas extravagantes, de certa forma conflituantes com o CPP, geram-se dificuldades na aplicação prática da lei. Para Correia (2014, p. 31), ao invés de "seguir o velho conselho iluminista de optar por poucas leis, simples e claras, o legislador escolheu a via incerta da pluralidade e da complexidade, gerando um sistema anárquico".

No subcapítulo seguinte temos a oportunidade de abordar alguma da dinâmica existente entre estes diplomas referidos anteriormente, for força de estudarmos a operacionalização das diferentes formas de obtenção de prova possíveis no decorrer das ações encobertas digitais.

3.4. Modi faciendi e (in)admissibilidade da prova obtida pelo agente encoberto digital

Tentaremos agora responder a duas questões que são objetivos centrais da presente investigação. Estas passam por entender quais os *modi faciendi* que podem ser adotados no

[36] Deputado do Partido Socialista.

decorrer das ações encobertas digitais para se efetuar a recolha de prova, e apreciar a admissibilidade destes, assim como das provas por estes recolhidas.

Na literatura[37] encontramos como possibilidades para atingir este desiderato que é a obtenção de prova pela via das ações encobertas digitais, a utilização de *malware*[38], de *hyperlinks*, de balizas de geolocalização, a criação de perfis falsos em plataformas como redes sociais e *chats* de conversação, o recurso a *cybercops* automatizados, e a drones. De seguida, individualizaremos cada um destes recursos, versando a admissibilidade, ou não, da prova por estes obtida.

A LCiber não tem qualquer norma especifica que mencione o modo de obter prova durante as ações encobertas ao abrigo desta, no entanto, diz-nos o n.º 2 do Art.º 19.º que, "sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção das comunicações". Esta norma é vaga e dá lugar a que a doutrina e a jurisprudência se pronunciem, havendo autores que consideram estar aqui patente a possibilidade de recurso à utilização de *malware* ou ainda às comumente designadas buscas *online.*

Para esta matéria, chamamos à colação a apreciação de Campos (2021), que se refere à LCiber como tendo ampliado à legislação processual penal novos meios de obtenção de prova, entre estes a utilização de *malware*, acrescentando que trouxe ainda a possibilidade de se adaptarem alguns já existentes para o ambiente virtual. Ainda assim, para a autora, deve-se afastar a utilização do *malware* "*ab initio*" (p. 81) do enquadramento previsto para as buscas do Art.º 174.º e ss. do CPP. A mesma menciona que, embora "se reduza a compreensão do *malware* a uma simples «busca», o «parâmetro» para aferir da sua previsão terá de ser a [LCiber], que incide sobre dados informáticos (os quais não são algo tangível ou corpóreo)" (p. 82), ao invés do estipulado no Art.º 174.º do CPP.

Campos (2021) defende igualmente que, limitando-se o *malware* a uma busca, e observando que a LCiber estabelece uma atividade "homónima" (p. 82) que é a «pesquisa de dados informáticos», é idóneo considerar o seu uso enquanto meio de obtenção de prova admissível, ao abrigo do Art.º 15.º da LCiber e Art.º 19.º da CCiber. Alicerça esta tese no

[37] Faremos, de seguida, a devida menção a cada um dos autores que tivemos em consideração.

[38] De acordo com Campos (2021, p. 27), o *malware* consiste num "programa informático que é instalado ocultamente no sistema informático do visado, para recolha de prova interna (dados armazenados, não armazenados ou produzidos em tempo real) e/ou prova externa ao sistema informático, quando aquele comporte a ativação de *hardware*". Ramos (2022) refere ainda que há doutrina que faz alusão a este tipo de *software* com designações tais como *trojan*, vírus, cavalo de troia ou *keylogger*. Campos (2001) acrescenta as designações *rootkits*, *spyware* e *worm*.

Ac. do TRP n.º 2039/14.0 JAPRT.P1, de 7 de julho de 2016, o qual refere nos parágrafos VII a IX que:

> A pesquisa no computador dos dados informáticos que dele constam, bem como a apreensão desses dados é regulada na Lei do Cibercrime, em cujo âmbito definido logo no artº 1º se encontram *"as disposições penais materiais e processuais (...), relativas ao domínio (...) da recolha de prova em suporte electrónico*".
>
> Apreendido um computador com acesso à internet, a autoridade judiciária pode ordenar ou autorizar a pesquisa desse sistema informático (artº 15º nº 1) e se no seu decurso foram encontrados dados ou documentos informáticos a autoridade judiciária ordena ou autoriza essa apreensão (artº 16º nº 1) - sem prejuízo da apreensão pela polícia criminal sujeita a validação (artº 16º nº 2 e 4), apreensão essa sujeita às formas do nº 7 do mesmo artº.
>
> Se, no decurso da pesquisa, for encontrado correio eletrónico ou registo de comunicações de natureza semelhantes, o juiz ordena ou autoriza a sua apreensão (artº 18º), seguindo-se o regime da apreensão de correspondência do CPP (artº 179º).

No que às ações encobertas em ambiente digital especificamente diz respeito, Campos (2021) aproxima-as da utilização do *malware*, na medida em que, segundo a autora, ambas têm "caráter oculto" (p. 94), pois nas ações encobertas digitais há ocultação da identidade do investigador e "no caso do *malware* há uma ocultação da instalação e funcionamento do programa no computador do visado" (p. 94).

No entanto, a autora considera que o *malware* é um meio de obtenção de prova autónomo pelo que não deve ser confundido nem legitimado ao abrigo do n.º 2 do Art.º 19.º da LCiber. Salienta ainda que "não poderia proceder-se à recolha de prova externa com recurso a *malware*, dado que o n.º 2 do artigo 19.º da [LCiber], que remete para o artigo 18.º, [faz] referência aos artigos 187.º, 188.º e 190.º, e não ao artigo 189.º do CPP, que trata dessa matéria" (p. 97).

Ramalho (2019), embora admitindo que a formulação "não é evidente" (p. 338), retira desta norma que é admissível no ordenamento jurídico o recurso a *malware*. Para o

autor trata-se "da consagração do *hacking*[39] e da utilização (que incluirá, naturalmente, a instalação) de *malware* como método oculto de investigação criminal em ambiente digital" (p. 346). Acrescenta que o legislador, ao não invocar outros meios de obtenção de prova típicos, quis "colmatar a insuficiência dos demais meios processuais existentes para abrangerem estes *meios e dispositivos informáticos*" (p. 344). Ressalva ainda que não se trata aqui dos "dispositivos eletromagnéticos, acústicos, mecânicos ou outros" referidos na definição de «interceção» da al. e) do Art.º 2.º da LCiber.

Não obstante, Ramalho (2013b) complementa que esta matéria carece de densificação legal, "porquanto, em medidas desta natureza, quase tão importante quanto a reserva de lei é a reserva de precisão legal" (p. 234). Para o autor, a "*ultima ratio*, mesmo dentro dos meios ocultos de investigação criminal, que está subjacente à utilização de *malware*, não se compadece com uma mera referência à sua necessidade", ou seja, com uma remissão para um outro regime.

Acompanhemos de seguida a linha de raciocínio de Ramalho (2013b). Para o autor, no decorrer de ações encobertas digitais, temos no Art.º 19.º n.º 2 da LCiber remissão para o estipulado no Art.º 18.º da mesma lei, ou seja, o regime da interceção das comunicações, quando houver recurso a meios e dispositivos informáticos. Ora, desse regime da interceção das comunicações do Art.º 18.º, faz-se nova remissão, desta feita, para o veiculado nos Art.ºs 187.º, 188.º e 190.º do CPP, ou seja, das escutas telefónicas.

Sabemos que as ações encobertas não são, - ou não devem ser -, do conhecimento dos arguidos, no entanto, o regime das escutas telefónicas, no Art.º 188.º n.º 8 do CPP e aplicável nestas ações, *ex vi* do Art.º 18.º n.º 4 da LCiber, prevê que a partir do encerramento do inquérito, "o assistente e o arguido podem examinar os suportes técnicos das conversações ou comunicações e obter (...) cópia das partes que pretendam transcrever para juntar ao processo, bem como dos relatórios (...) para requerer a abertura da instrução".

Destarte, o autor entende que com a primeira remissão do Art.º 19.º n.º 2 para o Art.º 18.º da LCiber, e consequente remissão para o regime das escutas telefónicas do Art.º 188.º do CPP, "poderemos cair no absurdo de não ser divulgada ao arguido a existência de uma ação encoberta" (2013b, p. 235), mas "de terem de lhe ser facultados os suportes técnicos nos quais se encontra armazenada a prova recolhida com recurso a *malware*, quando o uso

[39] De acordo com Brenner (2010), designa-se por *hacking* a utilização de um sistema informático com a intenção de obter acesso não autorizado a outros sistemas informáticos.

de *malware* apenas seria permitido no contexto de ações encobertas" (2013b, p. 235), que não podem ser reveladas.

Embora de uma outra perspetiva, Alves (2017) também defende que "o sistema processual penal português não prevê a possibilidade de se recorrer ao uso de *malware* como método oculto de investigação criminal" (p. 29). Para este, a "inegável" (p. 28) necessidade de um método de obtenção de prova como o *malware*, será admissível apenas quando expressamente consagrada na lei, o que não acontece nem no Art.º 15.º nem no Art.º 19.º da LCiber.

Por sua vez, Venâncio (2023) vai no sentido de serem aceites as buscas *online* no ordenamento jurídico pelo agente encoberto, pois sem mais delongas, refere que da remissão efetuada desde o Art.º 19.º n.º 2 da LCiber para o regime da interceção das comunicações do Art.º 18.º da mesma lei, resulta que "serão igualmente aplicáveis os procedimentos e pressupostos do regime das escutas telefónicas (...) sempre que for necessário recorrer a meios e dispositivos informáticos para levar a cabo essas ações encobertas" (p. 202).

Outros autores como Albuquerque (2011) e Nunes (2021), defendem que as denominadas buscas *online* estão previstas na lei, no entanto, ao abrigo do Art.º 15.º da LCiber, com a epígrafe "pesquisa de dados informáticos". Nunes (2021) divide mesmo as buscas *online* em dois tipos, a saber, as que se consubstanciam num acesso único, e aquelas que necessitam de se prolongar no tempo e, portanto, com maior danosidade para o visado. Já Albuquerque (2011), refere que as buscas *online* foram previstas pelo legislador na LCiber, no entanto, defende que este preceito normativo está ferido de inconstitucionalidade material, pois "permite que o MP e o OPC ordenem a pesquisa de um sistema informático, incluindo dados informáticos íntimos ou privados, sem o controlo prévio ou posterior da *pesquisa* por um juiz" (p. 502).

Com a devida vénia pelos autores citados, tendemos a concordar com a tese apresentada por Ramalho (2013b), na medida em que, averiguada a explicação deste relativamente à utilização de *malware* numa ação encoberta, não constatamos a precisão legal necessária para considerar tal meio de obtenção de prova. Já quanto à possibilidade de se fazerem buscas *online*, paralelamente às buscas em ambiente físico, ao abrigo do Art.º 174.º e ss. do CPP, concordamos com o defendido por Albuquerque (2011) e Nunes (2021), podendo estas serem feitas, *ex vi* do Art.º 15.º da LCiber, - e se ordenadas pelo JIC, acrescentamos nós -, ainda que não consideremos ser um dos métodos de obtenção de prova disponíveis no decorrer de ações encobertas digitais, porquanto não é necessário o requisito da ocultação da identidade.

Nesta senda, realizamos uma breve referência aos *hyperlinks*, pois são uma alternativa à utilização de *malware* no desígnio da identificação de determinados tipos de ilícitos criminais em ambiente digital, a qual tem a particularidade de não ser necessário conhecer previamente os suspeitos.

Esclarece Ramalho (2013b) que esta técnica é utilizada em países como os EUA, com o nome *hyperlink sting operations*, e a Itália, com a designação *siti civetta*. Embora com algumas adaptações entre ambos, devido às diferenças nos respetivos ordenamentos jurídicos, o objetivo é a deteção de práticas relacionadas com pornografia infantil. Esta técnica consiste na "criação e publicação, por parte das autoridades responsáveis pela investigação criminal, de *hyperlinks* que supostamente dariam acesso a conteúdo pedo-pornográfico" (2013b, p. 418) aos utilizadores.

Desta feita, Ramalho (2017) refere não ser possível fazer o *transfer* deste modo de obtenção de prova para o ordenamento jurídico português, pois, para além da "mera visualização ou posse de pornografia infantil não consubstanciarem, por si só, ilícitos criminais" (p. 309), afigurar-se-ia ofensivo para com a "integridade moral do visado e, como tal, encontrar-se-ia proscrito, desde logo por força do disposto nos artigos 1.º e 32.º n.º 8, da CRP" (p. 310).

Posto isto, abordaremos de seguida a utilização de balizas de geolocalização, com e sem recurso a dispositivos móveis, mencionadas por Ramos (2022) como podendo ser enquadradas enquanto meio de obtenção de prova no decorrer de ações encobertas digitais, em sede de investigação criminal. Estas balizas permitem aos OPC's saberem a localização exata do suspeito e ativar ferramentas no dispositivo (e. g. a câmara e o microfone).

Não obstante, o autor adianta desde logo que, ao contrário do ordenamento jurídico espanhol, de onde o próprio termo balizas é originário, em Portugal não é permitida a utilização deste método[40], ainda que também seja possível efetuar geolocalização com recurso a outras tecnologias.

Naquilo que diz respeito a esta temática, o Ac. do STJ n.º 7/10.0TELSB.L1.S1, de 8 de janeiro de 2014, veio criar confusão ao agregar várias destas tecnologias num mesmo conceito, cfr. parágrafo VI, onde se pode ler que:

> A obtenção de dados através da localização celular, muito em uso no meio militar e até civil, para controle da localização de pessoas, pela adaptação de um dispositivo

[40] *Ex vi* da declaração de inconstitucionalidade com força obrigatória geral dos Art.ºs 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho, cfr. Ac. do TC n.º 268/2022.

> (GPS ou GSM) ao telemóvel, diz respeito à utilização de dados, revela o percurso físico que o titular do telemóvel fez ou a está a fazer, a sua mobilidade ou permanência; por via da sua ligação à rede telefónica revela a localização do aparelho telefónico, obedecendo ao mesmo propósito que uma vigilância policial sobre um dado indivíduo potenciada pelos meios eletrónicos disponíveis pelas forças policiais, não permitindo aperceber ou revelar quaisquer comunicações nem o seu conteúdo.

Ramos (2022, p. 213) refere que, "a questão aflorada pelo STJ sobre a localização celular não é de fato uma verdadeira localização GPS". Nunes (2017) acrescenta que tem existido na doutrina e jurisprudência "uma acesa querela" (p. 98) quanto à admissibilidade de se utilizar a tecnologia GPS, desde que apenas para efeitos de se aferir a localização.

Destarte, o Ac. do TRE n.º 2005/08-1, de 7 de outubro de 2008, esclarece-nos que a localização celular funciona "quando é feita ou recebida uma chamada ou mensagem", e que a localização por GPS "é ativada por um aparelho sintonizado com pelo menos dois satélites, dos quais recebe a informação das coordenadas da longitude e da latitude a que o aparelho se encontra, fornecendo-lhe a localização do sítio exato". Assim, conclui que "localização por GPS não tem coisa alguma a ver com localização celular".

Para evidenciar esta diferença, salientamos as decisões do TRL[41], que, de acordo com Ramos (2022), negaram provimento ao MP quando este pretendia, em sede de investigação criminal, saber quem se encontrava em determinados locais e em determinados períodos temporais, através dos dados de tráfego das operadoras relativos a chamadas e mensagens dos clientes.

No que diz respeito à utilização de tecnologia GPS, estritamente para efeitos de aferir a localização dos indivíduos investigados, Ramos (2022) concorda com a utilização, defendendo que "numa vigilância o OPC poderá verificar com quem o seu alvo se encontrou, se transacionaram algum bem (...), na utilização de GPS apenas se constata à distância a posição (...), inexiste qualquer tráfego de comunicações ou de dados móveis" (p. 214). O Ac. do TRE n.º 2005/08-1, de 7 de outubro de 2008, complementa que "não carece de prévia autorização judicial o uso pelos [OPC´s] de localizadores de GPS colocados em veículos utilizados por pessoas investigadas em inquérito (e pelo tempo tipo por necessário pelo

[41] Cfr. Ac. do TRL n.º 131/14.0 JBLSB-A.L1-9, de 17 de dezembro de 2014; Ac. do TRL n.º 73/16.4 PFCSC-A.L1-5, de 3 de maio de 2016 e Ac. do TRL n.º 48/16.3 PBCSC-A.L1-9, de 22 de junho de 2016.

[OPC] encarregue do mesmo)". Cabral (2014) também admite a utilização deste meio de obtenção de prova enquanto método atípico à luz do Art.º 125.º do CPP, porquanto, refere, "não contende, ou contende apenas de forma superficial, com o direito à intimidade" (pp. 842-843).

Por sua vez, os autores Andrade (2009a) e Albuquerque (2011), defendem a inadmissibilidade deste método, considerando-o um método proibido de prova, devido ao fato de, uma vez que é atípico, não se encontrar devidamente previsto na lei, e ainda por ser altamente intrusivo para com a reserva da intimidade e da privacidade dos visados.

No que se cinge à utilização de balizas de geolocalização através de dispositivos móveis, concordamos com a sua inadmissibilidade enquanto método de obtenção de prova, *ex vi* do Ac. do TC n.º 268/22, de 19 de abril de 2022, que declarou padecerem de inconstitucionalidade as normas que permitiam a retenção e posterior acesso a esses dados[42]. Quanto à utilização de dispositivos GPS estritamente para se apurar a localização de indivíduos no decorrer de ações encobertas, tendemos a concordar com os autores Ramos (2022) e Cabral (2014), assim como do estipulado no Ac. do TRE n.º 2005/08-1, de 7 de outubro de 2008, que consideram a admissibilidade deste método de obtenção de prova.

Referimos anteriormente que a tecnologia das balizas de geolocalização permitem ativar ferramentas no aparelho, entre as quais a câmara e o microfone, pelo que está ainda a faltar verificar a admissibilidade da utilização deste recurso para registo de som e imagem. Não nos referimos à simples instalação de *malware* no aparelho para retirar dados, como abordado anteriormente, mas à sua instalação para a ativação remota destas funcionalidades no decorrer de ações encobertas digitais.

Não havendo nenhuma indicação neste sentido no RJAE nem na LCiber, chamamos à colação a Lei n.º 5/2002, de 11 de janeiro, que estabelece medidas de combate à criminalidade organizada e económico-financeira, sendo que esta, no seu Art.º 6.º n.º 1, admite o "registo de voz e imagem, por qualquer meio, sem consentimento do visado", para a investigação dos crimes constantes no seu Art.º 1.º. Após comparação dos crimes deste catálogo com os do RJAE e da LCiber, contata-se existirem alguns previstos em ambos, o que conjugado com a expressão "por qualquer meio", pode levar a crer que, pelo menos na investigação desses, se pode fazer uso desta ferramenta para obtenção de prova em ações encobertas digitais.

[42] Vd cap. 3.3.

Por conseguinte, Ramos (2022) elucida-nos que esta faculdade "não encontra amparo na [LCiber], para a realização de registos de voz e imagem" devido ao fato de o n.º 2 do Art.º 19.º referir expressamente que na necessidade de "recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção das comunicações". Ora, o autor refere que "não estamos na presença de uma situação de interceção das comunicações, mas sim na factualidade de verificar se é admissível ou não proceder à gravação de imagens e som ambiental (...) através de *benware*[43] instalado" (p. 220).

Desta feita, Andrade (2009b) e Ramos (2022) convergem no entendimento de que não se podem fazer escutas e gravações fonográficas no decorrer de ações encobertas digitais, por serem formas de devassa que não se encontram previstas e carecem de reserva de lei. Concordamos com os argumentos apresentados pelos autores e não encontramos na doutrina e jurisprudência argumentos contrários a estes.

Como já vimos, o RJAE, para o qual o Art.º 19.º da LCiber remete os termos do recurso às ações encobertas, apenas faz referência, no que diz respeito a procedimentos práticos, à faculdade de os agentes utilizarem identidade fictícia no decorrer destas. Fazendo uma analogia entre um ambiente a investigar físico e um ambiente a investigar digital, temos que um dos modos de obter prova por via das ações encobertas digitais, será a ocultação da verdadeira identidade por via da utilização de perfis falsos em plataformas como redes sociais ou *chats* de conversação, como, aliás, já mencionámos na presente investigação.

Ramalho (2017) divide esta tipologia de ações encobertas digitais com recurso a ocultação da verdadeira identidade em três conjuntos, a saber, (a) com "permanência ou interação pública em *chats*, fóruns, *websites* ou *blogs* acessíveis mediante registo prévio (ainda que não controlado)" (p. 294), (b) com "interação privada diretamente com indivíduos determinados, através do uso de janelas privadas de conversação, *e-mails*, *chats* privados ou outras formas" (p. 294), e, por fim, (c) com "infiltração em estruturas organizadas dedicadas à prática de crimes" (p. 294). Para Silva (2016), existem também três diferentes tipologias relativamente às informações obtidas nas redes sociais, que denomina por "informações/conversas públicas, restritas e privadas" (p. 3) que, na nossa opinião, acabam por confluir no mesmo, conforme veremos de seguida.

[43] O autor defende que, para efeitos de obtenção de prova em investigação criminal, ao invés de se utilizar o termo *malware*, que é a conjugação das palavras *malicious* com *software*, se deve utilizar o termo *benware*, substituindo desta feita a palavra *malicious* por *benign*.

Face às características que Ramalho (2017) atribui aos dois primeiros grupos citados, chamamos à colação o conceito de *Open Source Intelligence* (OSINT), que Gibson (2014) define como sendo "a exploração de dados e informações que estão legalmente disponíveis no domínio público" (p. 123). Goldman (2006) acrescenta a este conjunto de dados disponíveis para a generalidade do público, "os dados e informações de acesso limitado ou restrito, que implicam, por exemplo, um pagamento para serem acedidas" (p. 104).

De acordo com Ramalho (2017), a interação social na internet é diferente da do ambiente físico, na medida em que é normal "os cibernautas identificarem-se por *usernames* ou *nicknames* nas suas interações, independentemente da licitude dos propósitos", pelo que, a regra é ocultar a identidade em "fóruns, *chats*, *blogs* ou outros *websites*" (p. 293). Ramos (2022) acrescenta existir na internet para cada utilizador o que comumente se denomina por "pegada digital" (p. 162). Isto, porque tudo o que é publicado é de difícil reversão, sendo possível hodiernamente recuperar qualquer publicação de qualquer plataforma, mesmo que o criador pense tê-la apagado definitivamente. Segundo o autor, com recurso a OSINT, a investigação "fica facilitada pelos OPC's por a mesma ser realizada à distância e permitir um cruzamento de informação mais célere entre as diversas pesquisas que se efetuam" (p.163).

Para Ramos (2022) não há dúvidas quanto à legalidade de polícias recorrerem à internet para efetuarem pesquisas em fontes abertas sobre determinados indivíduos que investigam. Nunes (2021) considera que, neste ambiente, o agente "pode perfeitamente manter o seu anonimato e dificilmente correrá perigo", pelo que "bastará a criação de um *nickname*" (p. 467).

No que concerne ao primeiro dos conjuntos referidos por Ramalho (2017), apenas é necessário ao agente encoberto, para entrar nos locais e assistir livremente ao que lá se passa, criar um "nome fictício, que mais não é do que uma aparência virtual, análoga à aparência física ou à roupagem que o agente não identificado veste quando entra numa sala onde saiba que são praticados factos criminosos" (p. 295). Corresponde, portanto, ao recurso a OSINT, onde não existe qualquer tipo de violação de acessos condicionados para se chegar às fontes da informação (Ramos, 2022).

No entanto, o autor afirma poder ser mais discutível, eventualmente, se os polícias podem "criar perfis nas redes sociais, usando um nome fictício e fotos de perfil de outras pessoas para investigar um suspeito, enviando-lhe um «pedido de amizade»" (p. 166).

Como ponto de partida para responder a estas questão, Valente (2010) salienta desde logo que o motivo de se conceder uma identidade fictícia aos agentes não é o de defraudar a confiança dos suspeitos, mas sim a segurança dos primeiros, evitando represálias posteriores.

Quanto a este tema, Ramalho (2013a) defende que "não faz qualquer sentido a remissão para o regime de atribuição de identidade fictícia ao agente encoberto, previsto no Art.º 5.º da Lei n.º 101/2001, de 25 de agosto, quando a ação encoberta decorra em ambiente digital" (p. 408), pois desta forma, sempre que há necessidade da criação de um perfil falso numa rede social como o *facebook*, o *instagram*, ou outras, será necessário proferir despacho do Ministro da Justiça, mediante proposta do diretor nacional da PJ. Para Nunes (2021), que conflui no mesmo sentido, "bastará a criação de um *nickname*, que, como é óbvio, não carece de ser atribuído pelo [Ministro da Justiça]" (p. 467).

Não obstante, Ramalho (2017) acrescenta que, sendo desta forma, e não havendo normas legais específicas, deve então a AJ determinar "limites à criação destas *identidades virtuais*, não só evitando a utilização de nomes excessivamente sugestivos[44], mas também prevendo a possibilidade de, no perfil falso, ser introduzida uma fotografia de outrem" (p. 306).

De acordo com Ramos (2022), "maior controvérsia poder-se-á encontrar no que diz respeito às provas que se encontram protegidas nas redes sociais", ainda que considere continuarem a ser provas obtidas em fontes abertas, porquanto "o suspeito é livre de aceitar ou recusar o referido pedido de «amizade»", não havendo sujeição a qualquer tipo de "coação" (p. 173).

No mesmo sentido, ainda que com referência concreta para o caso da rede social *facebook*, pode ler-se nos parágrafos I e VIII do Ac. do TRL n.º 431/13.6 TTFUN.L1-4, de 29 de setembro de 2014, que:

> No conceito de "amigos" do Facebook cabem não só amigos mais próximos, como também outros amigos, simples conhecidos ou até pessoas que não se conhece pessoalmente, apenas se estabelecendo alguma afinidade de interesses no âmbito da comunicação na rede social que leva a aceitá-los como "amigos".

[44] Relativamente a isto, Mata (2011) salienta ser importante o agente encoberto certificar-se de que não induz alguém a perpetrar determinada conduta ilícita cuja intenção não tinha a inicialmente, para não se cair na «provocação», cuja separação entre ambos poderá ser mais ténue no ambiente digital do que no físico.

> Assim, está claramente afastado o carácter privado do grupo e a natureza "privada" ou "pessoal" das publicações e, logo, aquele conteúdo (post) e o seu autor não beneficiam da tutela da confidencialidade.

Por sua vez, Valente (2019) defende que a recolha "efetuada numa rede aberta ou aberta restrita ou fechada, porque o cidadão escreveu ou disponibilizou um vídeo autoincriminatório, não colhe nem deve num estado democrático de direito ser admitida" (p. 621), exceto se servir para comunicar a notícia de um crime às autoridades competentes. Para o autor, "podemos estar perante uma clara proibição de prova, nos termos do artigo 126.º, n.ºs 1 e 3 do CPP e artigo 32.º, n.º 8 da CRP, uma vez que as relações de confiança e lealdade social e pessoal assentam num esquema engenhoso de engano" (p. 621).

Ramos (2022) concorda com o Acórdão, o qual complementa dizendo que "estamos, na realidade, na presença de fontes abertas da investigação, que deverão ser usadas com a finalidade da descoberta da verdade material" (p. 174). Não obstante, acrescenta ainda que o fato de "um agente efetuar um «patrulhamento» a um local ou *site* da internet não configura uma ação encoberta, nos termos definidos no RJAE, uma vez que uma simples ação de investigação, consistindo numa vigilância disfarçada, não poderá ter esta qualificação" (p. 174).

Nunes (2021) tem diferente opinião neste aspeto, pois refere que "no plano informático-digital, a conduta do agente encoberto poderá consistir no «patrulhamento» de sítios da Internet, *chats* ou *newsgroups* abertos ou acedidos com o consentimento de um dos participantes" (p. 439).

Posto isto, chamamos agora à colação o segundo dos conjuntos referidos por Ramalho (2017), no qual já existem situações em que "o agente interage, em privado e, em certos casos também em público, diretamente com indivíduos determinados", não havendo apenas interação com meros presumíveis meliantes, mas também, com "aqueles em que o agente apenas inicia o contacto porque conhece a correspondência entre a identidade física e a virtual do visado" (p. 297). Quanto a estas situações, o autor salienta que o agente encoberto se apresenta perante o suspeito conotado com determinada conduta criminosa, e que as conversas provindas desta sua conduta dissimulada, enquanto meio de prova, justificam a "danosidade social" (p. 298) eventualmente provocada.

Por último, o terceiro dos conjuntos referidos por Ramalho (2017), "corresponde à infiltração do agente em estruturas organizadas dedicadas à prática de crimes", nas quais

inclui como exemplos "os *websites* dedicados à troca e comercialização de pornografia infantil, de tráfico de pessoas, de venda de armas, de venda de serviços de *hacking*, ou mesmo a organizações dedicadas à prática de crimes de contrafação" (p. 298).

No que diz respeito à utilização de perfis falsos para efeitos de investigação criminal pelas polícias no ordenamento jurídico português, Ramos (2022) afirma inexistir "qualquer discussão jurídica sobre esta situação" (p. 168), não havendo também ainda decisões de tribunais superiores.

No que concerne à recolha de informações em OSINT, sem qualquer interação com outros usuários, consideramos não se enquadrar naquilo que são ações encobertas digitais, conforme defendido por Ramos (2022), não havendo, de igual modo, nada que obste a tal procedimento por parte dos OPS's em sede de investigação criminal ou outra, conforme autores como Ramalho (2017), Nunes (2021) e Ramos (2022). Destarte, não para efeitos de investigação criminal, mas sim na produção de informações com o fim de salvaguardar a independência e defesa nacionais, o SIS e o SIED fazem este tipo de pesquisas em fontes abertas (Pereira, 2004).

Se, por sua vez, for necessário criar perfis falsos para aceder às contas restritas dos visados, através dos denominados pedidos de amizade, ainda que sem outro tipo de interação, concordamos com o estipulado no Ac. do TRL n.º 431/13.6 TTFUN.L1-4, de 29 de setembro de 2014, no sentido de continuarem a ser consideradas fontes abertas.

Quanto à interação com suspeitos através de perfis falsos por parte dos OPC's, vimos por Ramos (2022) não existir ainda discussão jurídica, pelo que, desta feita, tendemos a considerar que a analogia entre os ambientes físico e digital permitem uma remissão para o regime de atribuição de identidade fictícia ao agente encoberto, previsto no Art.º 5.º da Lei n.º 101/2001, de 25 de agosto, quando a ação encoberta decorra em ambiente digital, que será legal sempre que cumpra os normativos estabelecidos. Concordamos também com o mencionado por Ramalho (2017), que defende que a AJ deve definir regras precisas para esta utilização.

No seguimento da abordagem à utilização de perfis falsos no decorrer das ações encobertas digitais, fazemos agora uma breve referência aos denominados *cybercops*. Estamos a referir-nos, de acordo com Nunes (2021, p. 430), a "programas informáticos que simulam pessoas reais sem que quem esteja a interagir com estas pessoas virtuais se aperceba de que não se trata de uma pessoa verdadeira".

Como vimos anteriormente, o n.º 2 do Art.º 1.º do RJAE diz-nos que são consideradas como ações encobertas "aquelas que sejam desenvolvidas por funcionários de investigação

criminal ou por terceiro atuando sob o controlo da [PJ]". Uma vez que, desta feita, não nos estamos a referir a pessoas, mas sim a programas informáticos automatizados, impera a questão acerca da admissibilidade da prova assim obtida.

Entende Nunes (2021), "que nada na nossa Lei impede a utilização de *Cybercops* (pelo que as provas obtidas são lícitas e utilizáveis)" (p. 431), não colhendo o argumento da impossibilidade em razão de não serem efetuadas por pessoas «físicas». Defende a sua tese acrescentando que, "desde que o *Cybercop* seja controlado pelas autoridades, diretamente ou mediante o controlo do particular que controla o *Cybercop* ([e. g.], uma empresa que produza esses programas informáticos), não vemos em que medida a Lei não é observada" (p. 432). Embora não aludindo diretamente à utilização de *cybercops*, Ramalho (2017), refere que "poderá o agente nem sequer estar à frente do computador durante a sua atividade, limitando-se a gravar tudo o que é dito num *chat* ou o que ocorre num *website*" (pp. 295-296).

Por sua vez, Ramos (2022) é da opinião de que as provas obtidas através deste recurso não são válidas, evidenciando o argumento de não serem estas ações encobertas efetuadas por pessoas verdadeiras. Apesar disto, o autor acrescenta que "o caminho da investigação na internet vai passar obrigatoriamente pela inclusão de *cybercops* que irão realizar diligências de investigação na internet, sob diversas formas, na qual se inclui a do agente encoberto" (p. 227).

Na nossa opinião, e atendendo à interpretação da lei escrita, tendemos a concordar com a tese defendida por Ramos (2022), na medida em que, conforme está estipulada a remissão que o Art.º 19 da LCiber faz para o RJAE, não tem em atenção, *per si*, a este tipo de contingências do ambiente digital.

Uma última possibilidade que apresentamos enquanto método para obtenção de prova utilizado pelo agente encoberto digital é o recurso a drones no decorrer das ações.

Dwyer-Moss (2018) refere, relativamente a esta temática, que com o despertar de curiosidades e como resultado da evolução e maturação tecnológica, os drones começaram a ter um campo de aplicação mais alargado, pelo que, hodiernamente, estes dispositivos assumiram uma proliferação crescente na sociedade civil. Ramos (2022) complementa que este instrumento já é mesmo utilizado pelas polícias para reconhecimento de locais, para fins preventivos e também de investigação criminal.

De modo a apreciarmos a admissibilidade da prova obtida por este meio em ações encobertas digitais, verifiquemos primeiro as funcionalidades que esta tecnologia faculta. De acordo com Ramos (2002), para além de possibilitar fazer o reconhecimento de locais e

gravar imagens, também pode ser utilizada para "disseminar *benware* com o intuito de conseguir entrar nos sistemas informáticos de um suspeito" para recolher meios de prova, através da aproximação encoberta à "rede *wifi*" do mesmo (pp. 223-224).

Posto isto, e em primeiro lugar, enquadramos o procedimento de aproveitar a facilidade de aproximação facultada pelos drones a determinados locais, com o objetivo de disseminar *software* para obter dados dos suspeitos, no anteriormente observado para o uso de *malware*, pelo que não pode ser considerada admissível à luz do ordenamento jurídico a prova assim obtida.

No que respeita à recolha de imagens pelos drones, não existe ainda legislação nem jurisprudência relativamente a esta, enquanto meio de obtenção de prova penal. Desta feita, considerando apenas a recolha de imagens, concordamos com o argumento apresentado por Ramos (2022), para o qual se podem fazer, ainda que com "algumas reservas" (p. 222), de entre estas não serem obtidas mediante intromissão na vida privada. O autor sustenta a sua tese, por analogia, com o Ac. do TRE n.º 2005/08-1, de 7 de outubro de 2008, que decidiu no mesmo sentido, mas relativamente à utilização do GPS.

A simples captação de imagens na via pública ou em espaços abertos ao público tem vindo a ser comummente aceite pela jurisprudência, desde que exista proporcionalidade quanto à causa para a sua obtenção. Salientamos o Ac. do TRC n.º19/11.6 TAPBL.C1, de 10 de outubro de 2012, no qual se pode ler que "não constitui crime a obtenção de imagens, mesmo sem consentimento do visado, sempre que exista *justa causa* para tal procedimento, designadamente quando as mesmas estejam enquadradas em lugares públicos, visem a proteção de interesses públicos, ou hajam ocorrido publicamente". O Ac. do TRP n.º 349/13.2 PEGDM.P1, de 25 de fevereiro de 2015, complementa ainda que "nessas circunstâncias mesmo que haja falta de licenciamento da Comissão Nacional de Proteção de Dados (CNPD) podem ser usadas como meio de prova".

Por último, no respeitante à utilização de drones para efeitos de vigilância de suspeitos ou reconhecimento de locais (e. g. alvos de busca), somos também da opinião de Ramos (2022), que refere estarmos perante a "extensão de uma observação" (p. 222), que poderia ser efetuada por quaisquer outros polícias, mesmo apeados.

Para encerrar este périplo pelos *modi faciendi* das ações encobertas digitais, Ramalho (2017, p. 354) expõe que foi num "contexto de fragmentariedade e de assistematicidade" relativamente aos métodos de investigação criminal de natureza oculta, "que o legislador *enxertou* a prova digital, deixando ampla margem para a dúvida e incerteza na sua aplicação prática, em particular no plano operacional, cuja regulamentação permanece por realizar"

(p. 354). Defende o autor que se devem consagrar devidamente na lei estes "métodos de obtenção de prova mais invasivos que permitam fazer face a um novo tipo de criminalidade, que, de outro modo, permanecerá indetetável" (p. 355).

De acordo com Nunes (2021), este tipo de ações encobertas restringe vários direitos fundamentais, nomeadamente no que respeita à "intimidade/privacidade, à autodeterminação informacional, à confidencialidade e à integridade dos sistemas técnico-informacionais, à inviolabilidade do domicílio (embora apenas quando implique a entrada num espaço que goze da tutela deste direito) e à liberdade de expressão" (pp. 453-454). Complementa Valente (2019), que as ações encobertas digitais são "um dos meios de obtenção de prova mais ocultos, intrusivos e lesivos dos direitos fundamentais pessoais: [e.g.], reserva da intimidade da vida privada e familiar" (p. 616).

Para o autor, é essencial ter em atenção que "a verdade material não é um valor supremo, contrariamente à dignidade da pessoa humana, à integridade, à liberdade de pensar e conhecer sem qualquer coação, interpelação, coação" (p. 602). Neste propósito que é a busca da verdade material, Silva (2020) refere ainda que "é necessário ter presente que a verdade no processo não pode procurar-se por quaisquer meios, mas tão só pelos meios processualmente admissíveis, ainda que dessa limitação possa resultar algumas vezes o sacrifício da verdade" (p. 100). Opinião colhida por Antunes (2017), que acrescenta ser essencial, desde logo, ter em atenção o método de obtenção de prova utilizado.

Em suma, e conforme autores como Albuquerque (2011), Andrade (2013) e Valente (2019), estes métodos ocultos de obtenção de prova, por serem atípicos, devem estar previstos expressamente na lei, pois enquanto não estiverem devidamente esclarecidos os termos relativos à atuação destes, existirá lugar a dúvidas, o que não pode suceder.

Conclusão

E eis que chegou o momento de terminar o presente trabalho, pelo que apresentaremos nestas últimas linhas, alicerçados na legislação, doutrina e jurisprudência estudadas, as principais ideias chave que advieram do que nos propusemos investigar.

Para contextualizarmos o objeto de estudo, - e que serviu também como termo de comparação necessário -, trouxemos para a nossa mesa de trabalho, em primeiro lugar, as ações encobertas tradicionais, ou seja, em ambiento físico. Assim, chegamos ao motivo de terem surgido, como surgiram, o que são, e em que moldes se fazem. Ora, as mesmas tiveram o seu primeiro vislumbre no ordenamento em 1983 por via da então denominada «Lei da droga», como meio excecional de investigação perante um flagelo que proliferava na altura, e em 2001 foi criado o RJAE, lei extravagante que estabeleceu as normas pelas quais se rege este meio de obtenção de prova.

Todavia, quando o legislador trouxe para o ordenamento jurídico um regime geral com a possibilidade de recurso a este meio de prova atípico, o contexto criminal era diferente do atual. Hodiernamente, muita da criminalidade desterritorializou-se e, para além disso, deixou também de ter um rosto visível. Como pudemos ver, há miríades possibilidades de perpetrar crimes, tanto da casa ao lado das vítimas, como desde um país longínquo ao destas. Isto, através da utilização de computadores, *smartphones* ou *tablets* com acesso a redes como a internet. Desta feita, tanto as polícias como outros operadores do direito, tiveram de se adaptar, transversalmente em diferentes ordenamentos jurídicos um pouco por todo o mundo. Uma das reformas foi, em alguns destes, a possibilidade de se passarem a fazer as referidas ações encobertas, doravante em ambiente digital.

Em 2009, a LCiber transpôs para o âmbito nacional a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à CCiber do Conselho da Europa. Esta lei trouxe para o âmbito nacional a possibilidade de, em sede de investigação criminal, e de entre um catálogo de crimes, se fazer recurso às ações encobertas como resposta à cibercriminalidade, pela via do seu Art.º 19.º.

Destarte, o primeiro dos objetivos deste estudo passava por procurar responder se é uma norma da LCiber, que remete para o regime geral do RJAE, bastante para se efetuarem ações encobertas em ambiente digital. Ou de outra forma, se a lei positivada é, *per si*, suficiente para se atingir este desiderato. Não nos cabe tecer comentários ao RJAE, pois não é objeto central da presente investigação, e é relativo, *ab initio*, às ações encobertas efetuadas

pelos agentes no terreno físico. Todavia, não julgamos a remissão existente ser a mais correta forma de fazer o *transfer* desta importante ferramenta de investigação para o ambiente digital, devido não só à evolução e particularidades da tecnologia, mas porque as diferenças entre ambas as realidades são evidentes, e. g. a inadaptabilidade legal existente perante o recurso a *cybercops*, pois, atendendo à interpretação da lei escrita, não é tido em conta este tipo de contingências do ambiente digital. Posto isto, consideramos existir necessidade de uma redefinição.

Ficou patente pelo observado da discussão conjunta da reunião plenária que levou à sua aprovação, que com a LCiber o legislador tinha a melhor das intenções quanto ao "ataque" ao fenómeno da cibercriminalidade. Não obstante, passados catorze anos, e com manifesta necessidade crescente de perpetrar este mesmo combate, naquilo que à utilização da figura do agente encoberto digital em específico diz respeito, reforçamos ser momento de alterar o modelo legal quanto a esta matéria.

Constatamos não existir na jurisprudência, doutrina e na própria legislação, consenso quanto ao conceito dado ao ambiente em que ocorre o fenómeno da cibercriminalidade. Observam-se, hodiernamente, termos como "ambiente virtual", "ambiente digital", ou "ciberespaço", quando se depreende que se está a fazer referência ao mesmo. Relativamente a esta tipologia de crimes, *stricto sensu*, ora se faz alusão aos "crimes informáticos" ora aos "cibercrimes". A revogada Lei n.º 109/91, de 17 de agosto, começou por se referir a estes como sendo crimes informáticos, por seguir a direção dos ventos terminológicos das normativas da UE. Posteriormente, a LCiber tomou igual rumo.

O mesmo é extensível ao conceito da prova obtida neste, e por este meio. Na LCiber denomina-se por "prova em suporte eletrónico" e no CPP por "prova guardada em suporte digital", encontrando-se na doutrina e jurisprudência ainda os conceitos de "prova digital", "prova eletrónica" ou ainda prova "eletrónico-digital".

O segundo objetivo deste estudo passava por delimitar o conceito de ambiente digital perante outros conceitos, num desígnio de compreender se as denominações «agente encoberto digital» ou «ações encobertas digitais» são adequadas. Verificamos que, relativamente a esta tipologia de ações encobertas, é unânime[45] a utilização dos termos, ao que acrescentamos que a utilização do termo «prova digital» também é acolhido por maioria de razão. Ainda assim, não podemos deixar de referir que, esta desordem concetual, *per si*,

[45] Referimo-nos a unanimidade quanto aos termos «digital» ou «digitais», pois como observado no cap. 1.2, a doutrina e jurisprudência não são igualmente unânimes no que diz respeito ao termo «encoberto», havendo quem defenda o termo «infiltrado».

pode levar a que processos futuros venham a ser inquinados, pelo que, na nossa opinião, se deve procurar uma unificação.

Notamos que, maioritariamente, a legislação portuguesa em matéria de cibercriminalidade, tem passado sempre pela transposição de diplomas oriundos das altas instâncias europeias, ora via decisões-quadro ora diretivas. Consideramos tratar-se, por isso, de uma miscelânea de normas, opinião atestada pela jurisprudência, pois em algumas matérias já vai até em sentidos distintos. Deste modo, recomendamos existir uma de duas opções a seguir, que passam, ou por transpor para os CP e CPP todas as outras normas que dizem respeito à recolha de prova em ambiente digital, ou então, condensá-las num único diploma, contendo todo o direito substantivo e adjetivo relativamente a esta temática.

Neste estudo que agora concluímos, dois outros objetivos, - indissociáveis -, passavam por apurar quais os *modi faciendi* que podem ser adotados no decorrer das ações encobertas digitais, para efetivamente se realizar a recolha de prova, apreciando sempre a admissibilidade destes e da respetiva prova assim obtida. Ora, não encontrando nós qualquer estandardização quanto às fontes, surgiram como resultados desta pesquisa na doutrina relativamente a este desiderato, a utilização de *malware*, de *hyperlinks*, de balizas de geolocalização, a criação de perfis falsos em plataformas como redes sociais e *chats* de conversação, o recurso a *cybercops* automatizados, e a drones.

Se, por ventura, se efetuar uma analogia com o estipulado no RJAE, e se constatar que este também não tem normas específicas que contenham os diversos modos de atuação e respetiva obtenção de prova no decorrer das ações encobertas em ambiente físico, devemos ter em conta as particularidades da prova digital e respetiva recolha. Defendemos que a obtenção desta requer uma correspondente especificação em campos próprios, quer substantiva, quer adjetivamente, ainda mais no que às ações encobertas diz respeito.

No que concerne à admissibilidade da prova por via dos *modi faciendi* estudados, contatamos não haver, nem na doutrina nem na jurisprudência, total conformação quanto aos mesmos. Acrescentamos até que não encontramos nenhuma decisão de tribunais superiores relativamente ao recurso às ações encobertas digitais, pelo que a abordagem feita pela jurisprudência não se refere nunca a estas em concreto, mas a aplicações semelhantes.

Posto isto, chegamos ao momento em que é oportuno responder à pergunta de partida a que nos propomos como objeto de estudo: «no ordenamento jurídico português, é clara a admissibilidade da prova obtida em contexto de investigação criminal pelo agente encoberto em ambiente digital?». Tendo em conta o estudo que agora damos por finalizado, viemos a

concluir não ser clara no ordenamento jurídico português, a admissibilidade da prova obtida em contexto de investigação criminal pelo agente encoberto em ambiente digital.

Salientamos que no respeitante à utilização de perfis falsos em plataformas como redes sociais e *chats* de conversação, efetuada a devida analogia para com a utilização de identidade fictícia ao abrigo do RJAE no decorrer de ações encobertas em ambiente físico, se no segundo a doutrina e jurisprudência não têm dúvidas quanto à delimitação entre ações provocatórias e encobertas, já quanto ao primeiro, verifica-se ser muito ténue esta mesma delimitação. O novo paradigma envolto na interação entre utilizadores que o ambiente digital trouxe, com características muito próprias, veio adensar estas dúvidas.

Evidenciamos também, naquilo que diz respeito à discussão da utilização de *malware* enquanto ferramenta possível no decorrer de ações encobertas digitais, existir tal disparidade doutrinal, que por vezes nem se diferencia da figura das denominadas buscas *online*, - com génese diferente. Quesito este que nos faz voltar novamente à LCiber, pois esta trouxe para o âmbito nacional novas formas de obtenção de prova, *ex vi* da ratificação da CCiber, no entanto as normas processuais não tiveram redações precisas, deixando a doutrina e jurisprudência com espaço para abordar as questões deixadas em aberto.

Uma dessas discussões é, precisamente, a recolha de prova digital. Tal como era expectável, esta corresponde à principal tipologia de prova recolhida de entre os diversos meios de obtenção, no decorrer de ações encobertas digitais. No entanto, esta tem especificidades *sui generis*, que solicitam um diferenciado tratamento na sua recolha e manuseamento, que por sua vez, também requer especiais conhecimentos por parte dos OPC's que o fazem, quer sejam estas efetuadas no decorrer de ações encobertas digitais ou não. Por conseguinte, outro dos objetivos do presente estudo passou por apurar em que moldes legais se faz a obtenção da prova digital, uma vez que esta regulação é difusa. Ademais, desde que idealizamos as linhas de investigação para o presente trabalho, sucedeu a declaração de inconstitucionalidade, com força obrigatória geral, de normas da Lei n.º 32/2008, de 17 de julho, e como resposta possível para tal modificação na ordem jurídica, a respetiva alteração à Lei n.º 41/2004, de 18 de agosto.

Existia, relativamente à obtenção desta prova, uma articulação legal entre a LCiber, os Art.ºs 187.º a 190.º do CPP e a Lei 32/2008, de 17 de julho. Entretanto substitui-se esta última pela versão mais recente da Lei n.º 41/2004, de 18 de agosto. Desta articulação, para além de muitas outras questões que vale a pena aprofundar futuramente, não existe qualquer destrinça entre os métodos de intervenção das ações encobertas para outros. Surgiu então a

seguinte questão: «se é assim, porque se criou a norma relativa às ações encobertas digitais?». Não conseguimos encontrar a resposta.

Para finalizar, mesmo que a obtenção de prova pela via de métodos ocultos de investigação criminal como as ações encobertas digitais, ou outra, seja feita mediante o estrito cumprimento dos requisitos legais, não é por si só garante da sua validade. Para atingir o desiderato da admissibilidade da prova assim obtida, é necessária a análise de um conjunto de quesitos, tais como a necessidade, a adequação e a proporcionalidade, *stricto sensu*. Não deve, jamais, a verdade material sobrepor-se aos direitos, liberdades e garantias dos cidadãos, qual ingerência do estado perante estes. O caminho a trilhar para se obter prova admissível em processo penal por via das ações encobertas digitais ainda nos parece sinuoso, devendo resguardar-se das possíveis proibições de prova, de violar princípios constitucionais, ou ainda, de afetar direitos, liberdades e garantias do arguido, cabendo ao legislador tomar este rumo.

Apontamos como limitações ao trabalho que terminamos, em primeiro lugar, o fato de a figura do agente encoberto digital não ter ainda sido alvo de escrutínio, nomeadamente em tribunais superiores, pelo que não temos conhecimento dos moldes em que é, ou mesmo se é efetuada a sua aplicabilidade operacional. Passava por ser um dos nossos objetivos iniciais analisar jurisprudência acerca de casos reais desta aplicabilidade, pelo que, não sendo possível, nos ficamos pelo plano doutrinário. Em segundo lugar, salientamos o fato de termos verificado serem muitos os moldes em que esta tipologia das ações pode ser efetivada, estando as várias opções dispersas pela doutrina. Tornou-se, assim, uma tarefa árdua, a aglutinação e respetiva parametrização destes num único estudo, uma vez que se tratam de meios de obtenção de prova desiguais entre si.

Sugerimos para investigações futuras, alicerçados numa base de continuação relativamente ao que já foi feito, e destacando deste já a segunda das limitações por nós enunciada, o estudo individual de cada uma das opções que se encontram na doutrina. Desde logo, evidenciamos primeiramente a utilização de *malware* e de recurso a perfis falsos nas redes sociais e *chats* de conversação, por serem aqueles que maioritariamente têm cabimento para a sua utilização por parte das necessidades de investigação das polícias. Outra investigação futura que propomos corresponde ao estudo aprofundado da teia legal que existe em torno da recolha da prova digital no ordenamento jurídico português.

Referências

Acórdão de 10 de outubro de 2012. Processo n.º 19/11.6 TAPBL.C1. Tribunal da Relação de Coimbra. (Relator: Elisa Sales).

Acórdão de 14 de outubro de 1998. Processo n.º 578/98. Tribunal Constitucional. (Relator: Messias Bento).

Acórdão de 19 de abril de 2022. Processo n.º 268/22. Tribunal Constitucional. (Relator: Afonso Patrão).

Acórdão de 20 de fevereiro de 2003. Processo n.º 02P4510. Supremo Tribunal de Justiça. (Relator: Simas Santos).

Acórdão de 20 de janeiro de 2015. Processo n.º 648/14.6 GCFAR-A.E1. Tribunal da Relação de Évora. (Relator: João Gomes de Sousa).

Acórdão de 25 de fevereiro de 2015. Processo n.º 349/13.2 PEGDM.P1. Tribunal da Relação do Porto. (Relator: Maria Deolinda Dionísio).

Acórdão de 27 de junho de 2012. Processo n.º 127/10.0JABRG.G2.S1. Supremo Tribunal de Justiça. (Relator: Santos Cabral).

Acórdão de 29 de setembro de 2014. Processo n.º 431/13.6 TTFUN.L1-4. Tribunal da Relação de Lisboa. (Relator: Jerónimo Freitas).

Acórdão de 7 de julho de 2016. Processo n.º 2039/14.0JAPRT.P1. Tribunal da Relação do Porto. (Relator: José Carreto).

Acórdão de 7 de maio de 2014. Processo n.º 8292/12.6TDPRT.P1. Tribunal da Relação do Porto. (Relator: Lígia Figueiredo).

Acórdão de 8 de janeiro de 2014. Processo n.º 7/10.0TELSB.L1.S1. Supremo Tribunal de Justiça. (Relator: Armindo Monteiro).

Albuquerque, P. P. (2003). *A reforma da justiça criminal em Portugal e na Europa.* Almedina.

Albuquerque, P. P. (2011). *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem* (4.ª Ed.). Universidade Católica Editora.

Almeida, I. (2018). *A prova digital*. Librum Editora.

Alves, D. B. (2017). Uso de malware em investigação criminal. *Actualidad Jurídica Uría Menéndez*(47), pp. 19-30.

Alves, M. (2021). *Contingências e limites das ações encobertas: Necessidades e vindícia da investigação criminal* [Dissertação de Mestrado]. Instituto Superior de Ciências Policiais e Segurança Interna. https://comum.rcaap.pt/bitstream/10400.26/37060/1/Dissertação%20-%20Manuel%20Alves.pdf

Andrade, M. C. (2009a). «*Bruscamente no verão passado*»*: A reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia ter sido diferente.* Coimbra Editora.

Andrade, M. C. (2009b). Métodos ocultos de investigação (Plädoyer para uma teoria geral). In Monte, M. F., Calheiros, M. C., Monteiro, F. C. & Loureiro, F. N. (Coords.), *Que futuro para o Direito Processual Penal? Simpósio em homenagem a Jorge Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal português.* Coimbra Editora.

Andrade, M. C. (2013). *Sobre as proibições de prova em processo penal.* (Reimpressão). Coimbra Editora.

Antunes, M. & Rodrigues, B. (2018). *Introdução à cibersegurança: A internet, os aspetos legais e a análise digital forense.* FCA.

Antunes, M. J. (2017) *Direito processual penal.* Almedina.

Bauman, Z. (2005). *Confiança e medo na cidade.* Relógio D'Água Editores.

Beck, U. (1998) *La sociedad del riesgo: Hacia una nueva modernidad*. Editorial Paidós.

Beleza, T. P. & Pinto, F. L. C. (2013). A prova criminal e as garantias de defesa: Linhas de leitura e pontos de tensão. In Beleza, T. P. & Pinto, F. L. C. (Coords.), *Prova criminal e direito de defesa: Estudos sobre teoria da prova e garantias de defesa em processo penal* (2.ª reimpressão, pp. 5 e ss.)*.* Almedina.

Bentham, J. (2001). *Tratado de las pruebas judiciales*. Editorial Comares.

Braz, J. (2020). *Investigação Criminal. A organização, o método e a prova: Os desafios da nova criminalidade* (5ª Ed.). Almedina.

Brenner, S. W. (2010). Nanocrime? *University of Illinois journal of law, technology & policy, 2011*(1), pp. 34-105. https://illinoisjltp.com/journal/wp-content/uploads/2013/10/Brenner.pdf

Cabral, S. (2014). Art.º 189.º. In Gaspar, A. J., Cabral, S., Costa, E. M., Mendes, A. J. F. O., Madeira, A. P. & Graça, A. P. H. (Autores), *Código de processo penal: Anotado*. Almedina.

Campos, J. F. S. (2021). *O malware como meio de obtenção de prova em processo penal: A investigação oculta em ambiente digital*. Almedina.

Canotilho, J. J. G. & Moreira, V. (2007). *Constituição da República Portuguesa anotada* (4.ª Ed., Vol. I). Coimbra Editora.

Carrapiço, H. (2005). O crime organizado e as novas tecnologias: Uma faca de dois gumes. *Revista do Instituto da Defesa Nacional, (3)*111, pp. 175-192. https://comum.rcaap.pt/handle/10400.26/1156

Carta dos Direitos Fundamentais da União Europeia, de 7 de junho de 2016. *Jornal da União Europeia*. n.º C202/839. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT

Castells, M. (2005). *A galáxia internet: Reflexões sobre a internet, negócios e sociedade.* Fundação Calouste Gulbenkian.

Castro, E. (2012). *Agente infiltrado: Contributos para a compreensão da figura do terceiro* [Dissertação de Mestrado]. Instituto Superior de Ciências Policiais e Segurança Interna. https://comum.rcaap.pt/bitstream/10400.26/32169/1/Dissertação%20de%20Mestrado%20-%20Agente%20Infiltrado%28revista%29%20-%20Cópia.pdf

Catana, A. (2018). *A natureza jurídica da ação do agente infiltrado digital* [Dissertação de Mestrado]. Instituto Superior de Ciências Policiais e Segurança Interna. https://comum.rcaap.pt/bitstream/10400.26/25348/1/dissertação%20do%20agente%20infiltrado%20%28final%29%20pos%20defesa%20Versão%20II.pdf

Comissão das Comunidades Europeias. (2007). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das regiões: Rumo a uma política geral de luta contra o cibercrime*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52007DC0267&from=PT.

Convenção sobre o Cibercrime, de 23 de novembro de 2001. *European Treaty.* n.º 185. Conselho da Europa. https://rm.coe.int/1680081561

Correia, E. (2016). *Direito criminal II* (Reimpressão). Almedina.

Correia, J. C. (2014). Prova digital: As leis que temos e as leis que devíamos ter. *Revista do Ministério Público*(139), pp. 29-59.

Costa, E. M. (2014). *Ações encobertas: Alguns problemas, algumas sugestões.* FDUL.

Costa, J. F. F. (1998). *Direito penal da comunicação: Alguns escritos.* Coimbra Editora.

Coutinho, C. P. (2018). *Metodologia de investigação em ciências sociais e humanas: Teoria e prática* (2ª Ed.). Almedina.

Decisão do Tribunal do Ohio, de 30 de setembro de 1997. *Federal Supplement*. n.º 979. (United States v. Charbonneau). https://law.justia.com/cases/federal/district-courts/FSupp/979/1177/1446971/

Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de fevereiro. *Jornal Oficial da União Europeia*. n.º L 69/67. Conselho da União Europeia. (Relativa a ataques contra os sistemas de informação).

Decreto do Presidente da República n.º 91/2009, de 15 de setembro. *Diário da República.* Série I, n.º 179/2009, p. 6318. (Ratifica a Convenção sobre o Cibercrime).

Decreto n.º 10/04 de 1976. *Diário da República.* Série I, n.º 86/1976, pp. 737-775. Assembleia Constituinte. (Decreto de aprovação da Constituição).

Decreto-Lei n.º 22:992, de 29 de agosto. *Diário do Governo.* Série I, n.º 195/1933, pp. 1583-1585. Ministério do Interior. (Cria a Polícia de Vigilância e Defesa do Estado).

Decreto-Lei n.º 35:042, de 20 de outubro. *Diário do Governo*. Série I, n.º 233/1945, pp. 839-850. Ministério da Justiça. (Organiza os serviços da Polícia Judiciária).

Decreto-Lei n.º 35:046, de 22 de outubro. *Diário do Governo*. Série I, n.º 234/1945, pp. 857-859. Ministérios do Interior e da Justiça. (Cria a Polícia Internacional e de Defesa do Estado).

Decreto-Lei n.º 430/83, de 13 de dezembro. *Diário da República*. Série I, n.º 285/1983, pp. 4015-4029. Ministério da Justiça e da Saúde. (Altera o regime em vigor, tipifica novos ilícitos penais e contravencionais e define novas penas ou modifica as atuais em matéria de consumo e tráfico ilícito de drogas).

Decreto-Lei n.º 47344/66, de 25 de novembro. *Diário da República*. Série I, n.º 274/1966, pp. 1883-2086. Ministério da Justiça. (Aprova o Código Civil).

Decreto-Lei n.º 63/1985, de 14 de março. *Diário da República*. Série I, n.º 61/1985, pp. 662-689. Ministério da Cultura. (Aprova o código do direito de autor e dos direitos conexos).

Decreto-Lei n.º 78/87, de 17 de fevereiro. *Diário da República*. Série I, n.º 40/1987, pp. 617-699. Ministério da Justiça. (Aprova o Código de Processo Penal).

Descartes, R. (1989). *O discurso do método.* Martins Fontes Editora.

Despacho n.º 13692/2013, de 28 de outubro. *Diário da República*. Série II, n.º 208/2013, pp. 31976-31979. Ministério da Defesa Nacional. (Orientação para a política de ciberdefesa).

Dias, J. F. (2001). *Temas básicos da doutrina pena: Sobre os fundamentos da doutrina penal - sobre a doutrina geral do crime*. Coimbra Editora.

Dias, J. F. (2004). *Clássicos Jurídicos, Direito Processual Penal.* Almedina.

Dias, J. F. (2014). Por onde vai o Processo Penal Português - Por estradas ou por veredas? In *As conferências do Centro de Estudos Judiciários.* (pp. 49-88). Almedina.

Dias, J. F. (2016). Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal. In *Revista de legislação e jurisprudência, 146*(4000), pp. 3-16.

Dwyer-Moss, J. (2018). The sky government authorities: Drones and the fourth amendment. *Albany Law Review, 81*(3), pp. 1047-1070.

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

Fernandes, L. F. (2014). *Intelligence e segurança interna.* ISCPSI.

Ferreira, M. C. (2010). *Lições de direito penal* (4ª Ed.). Almedina.

Ferreira, V. D. (1996). Problémes posès par la mise en oeuvre des opérations undercover dans le domaine de la lutte contre la trafic de stupéfiants, *Revue de droit pénal et de criminologie, 76*(5), pp. 566-570. https://bib.kuleuven.be/rbib/collectie/archieven/rdpc/1996-5.pdf

Fijnaux, C. & Marx, G. (1995). *Undercover-police surveillance in comparative perspective.* Springer.

Gaspar, A. H. (2004). As ações encobertas e o processo penal: Questões sobre a prova e o processo equitativo. In Gaspar, A. H. (Ed.). *Medidas de combate à criminalidade organizada e económico-financeira* (pp. 43-53). Coimbra editora.

Gibson, S. D. (2014). Open Source Intelligence. In Dover, R., Goodman, M. S. & Hillebrand, C. (Eds.). *Routledge Compation to Intelligence Studies* (pp. 123-131). Routledge.

Gibson, W. F. (1984). *Neuromancer.* Ace Books.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social* (6ª Ed.) Editora Atlas.

Giuliani, A. (1971). *Il concetto di prova: Contributo alla logica giuridica*. Giuffrè.

Goldman, J. (2006). Words of intelligence: A dictionary. Scarecrow press.

Gómez, B. R. (2017). La infiltracíon policial em internet: A propósito de la regulación del agente encubierto informático en la ley orgánica 13/2015, de 5 de octubre, de modificacíon de la ley de enjuciamiento criminal para el fortalecimiento de las garantías procesales y la regulacíon de las medidas de investigación tecnológica. In López, M. F. (Coord.), *Justicia penal y nuevas formas de delincuencia* (pp. 98-123). Tirant to Blach.

Greco, L. (2003). O conceito de prova. *Revista da Faculdade de Direito de Campos, IV*(4), pp. 213-269. http://fdc.br/Arquivos/Mestrado/Revistas/Revista04e05/Docente/13.pdf

Ihering, R. V. (2009). *A luta pelo direito.* Martin Claret.

Jaramillo, A. D. R. (2010). *El agente encubierto frente a los derechos fundamentales a la intimidad y a la autoincriminación.* Universidad de Antiquoa.

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business horizons, 53*(1), pp. 59-68.

Knightley, P. (1990). *Espiões e espionagem: História da segunda mais velha profissão do mundo.* Círculo de Leitores.

Lakatos, E. M. & Marconi, M. A. (2003). *Fundamentos de metodologia científica* (5ª Ed.). Atlas S.A.

Larenz, K. (1997). *Metodologia da ciência do direito* (3ª Ed.). Fundação Calouste Gulbenkian.

Lei n.º 101/2001, de 25 de agosto. *Diário da República*. Série I-A, n.º 197/2001, pp. 5452-5453. Assembleia da República. (Regime jurídico das ações encobertas para fins de prevenção e investigação criminal).

Lei n.º 104/2001, de 25 de agosto. *Diário da República*. Série I-A, n.º 197/2001, pp. 5456-5457. Assembleia da República. (Aprova a lei da cooperação judiciária internacional em matéria penal).

Lei n.º 15/93, de 22 de janeiro. *Diário da República*. Série I-A, n.º 18/1993, pp. 234-252. Ministério da Justiça. (Revê a legislação de combate à droga).

Lei n.º 16/2022, de 16 de agosto. *Diário da República*. Série I, n.º 157/2022, pp. 2-137. Assembleia da República. (Aprova a Lei das Comunicações Eletrónicas).

Lei n.º 2/2023, de 16 de janeiro. *Diário da República*. Série I, n.º 11/2023, pp. 2-19. Assembleia da República. (Completa a transposição da Diretiva UE 2017/541, alterando a Lei de combate ao terrorismo, o Código Penal, o Código de Processo Penal e legislação conexa).

Lei n.º 23/2007, de 4 de julho. *Diário da República*. Série I, n.º 127/2007, pp. 4290-4330. Assembleia da República. (Aprova o regime jurídico da entrada, permanência, saída e afastamento de estrangeiros do território nacional).

Lei n.º 32/2008, de 17 de julho. *Diário da República*. Série I, n.º 137/2008, pp. 4454-4458. Assembleia da República. (Transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de

comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações).

Lei n.º 36/94, de 29 de setembro. *Diário da República*. Série I, n.º 226/1994, pp. 5908-5910. Assembleia da República. (Aprova a lei de medidas de combate à corrupção e criminalidade económica e financeira).

Lei n.º 41/2004, de 18 de agosto. *Diário da República*. Série I-A, n.º 194/2004, pp. 5241-5245. Assembleia da República. (Transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Concelho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas).

Lei n.º 49/2008, de 27 de agosto. *Diário da República*. Série I, n.º 165/2008, pp. 6038-6042. Assembleia da República. (Aprova a lei de organização da investigação criminal).

Lei n.º 5/2002, de 11 de janeiro. *Diário da República*. Série I-A, n.º 9/2002, pp. 204-207. Assembleia da República. (Estabelece medidas de combate à criminalidade organizada e económico-financeira).

Lei n.º 53/2008, de 29 de agosto. *Diário da República*. Série I, n.º 167/2008, pp. 6135-6141. Assembleia da República. (Aprova a lei de segurança interna).

Lei n.º 60/2013, de 23 de agosto. *Diário da República*. Série I, n.º 162//2013, pp. 5088-5090. Assembleia da República. (Transpôs para a ordem jurídica interna a Diretiva n.º 2011/36/UE, do Parlamento Europeu e do Conselho, de 5 de abril, relativa à prevenção e luta contra o tráfico de seres humanos e à proteção das vítimas).

Lei n.º 61/2015, de 24 de junho. *Diário da República*. Série I, n.º 121//2015, pp. 4412-4413. Assembleia da República. (Inclusão de todos os ilícitos criminais relacionados com terrorismo).

Lei n.º 88/2017, de 21 de agosto. *Diário da República*. Série I, n.º 160/2017, pp. 4856-4870. Assembleia da República. (Aprova o regime jurídico da emissão, transmissão, reconhecimento e execução de decisões europeias de investigação em matéria penal, transpõe a Diretiva 2014/41/EU, do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal).

Lei n.º 9/2007, de 19 de fevereiro. *Diário da República*. Série I, n.º 35/2007, pp. 1238-1252. Assembleia da República. (Estabelece orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança).

Lei n.º 93/99, de 14 de julho. *Diário da República*. Série I-A, n.º 162/1999, pp. 4386-4391. Assembleia da República. (Regula a aplicação de medidas para proteção de testemunhas em processo penal).

Lei nº 109/2009, de 15 de setembro. *Diário da República*. Série I, n.º 179/2009, pp. 6319-6325. Assembleia da República. (Aprova a lei do cibercrime).

Lempert, P. (2006). Caught in the web. *Progressive grocer, 85*(12), pp. 18 e ss.

Lusa. (2020, 11 de novembro). *Polícia desmantela rede mundial de pedofilia com centro na Austrália*. Público. https://www.publico.pt/2020/11/11/mundo/noticia/policia-desmantela-rede-mundial-pedofilia-centro-australia-1938741.

Martins, L. (2003). *Direito internacional da droga e da toxicodependência.* Coimbra Editora.

Mata, F. B. (2011, 2 e 3 de junho). *El agente encubierto em internet: Mentiras virtuales para alcanzar la justicia* [Los retos del poder judicial ante la sociedad globalizada]. IV congresso galego de Derecho Processal, La Coruña.

Matos, J. (2015). *O agente infiltrado como meio de obtenção de prova e consequentes danos na sociedade* [Dissertação de Mestrado]. Universidade Autónoma de Lisboa. https://repositorio.ual.pt/bitstream/11144/1843/1/Dissertação%20de%20Mestrado%201111.pdf

Meireis, M. A. A. (1999). *O regime das provas obtidas pelo agente provocador em processo penal.* Almedina.

Mendes, J. C. (2014). *Direito processual civil* (Vol. I). AAFDL Editora.

Mendes, P. S. (2004). As proibições de prova no processo penal. In Palma, M. F. (Coord.), *Jornadas de Direito Processual Penal e Direitos Fundamentais.* (pp. 132-133).

Mesquita, P. D. (2010). *Processo penal, prova e sistema judiciário.* Coimbra Editora.

Miranda, J. (2014). *Manual de direito constitucional: Direitos fundamentais - Tomo IV* (5.ª Ed.). Coimbra Editora.

Murray, J. (1997). *Hamlet on the holodeck: The future of narrative in cyberspace*. Simon and Schuster.

Neves, R. C. (2011). *As ingerências nas comunicações eletrónicas em processo penal.* Coimbra Editora.

Nogueira, M. J. (1998, 5 a 7 de novembro). *Polícias: Segurança; Investigação criminal; Limites* [Direitos humanos e eficácia policial: Sistemas de controlo da atividade policial]. Seminário internacional sobre direitos humanos e eficácia policial: Sistemas de controlo da atividade policial, Lisboa.

Novais, J. R. (2004). *Os princípios constitucionais estruturantes da República Portuguesa.* Coimbra Editora.

Nunes, D. R. (2017). A admissibilidade da obtenção, diretamente pelas autoridades, de dados de localização por meio de sistema GPS à luz do direito processual português. *Julgar*(32), pp. 97-122. http://julgar.pt/wp-content/uploads/2017/05/JLGR32-DARN.pdf

Nunes, D. R. (2021). *Os meios de obtenção de prova previstos na lei do cibercrime* (2.ª Ed.). Gestlegal.

Office of the Chairman of the Joint. (2021). *Dictionary of Military and Association Terms*. https://irp.fas.org/doddir/dod/dictionary.pdf

Oneto, I. (2005). *O agente infiltrado: Contributo para a compreensão do regime jurídico das ações encobertas.* Coimbra editora.

Palma, M. F. (2011, 18 de dezembro). Agente provocador. Correio da Manhã. https://www.cmjornal.pt/opiniao/detalhe/agente-provocador.

Palma, M. F. (2014). Introdução ao direito da investigação criminal e da prova. In Palma, M. F., Dias, A. S., Mendes, P. S. & Almeida, C. (Coords.), *Direito da investigação criminal e da prova.* (pp. 7-18). Almedina.

Palma, M. F. (2017) *Direito Penal. Conceito material de crime, princípios e fundamentos. Teoria da lei penal: Interpretação, aplicação no tempo, no espaço e quanto às pessoas* (2ª Ed). Faculdade de Direito de Lisboa.

Parecer de 16 de maio de 2002. n.º I001462001. Conselho Consultivo da Procuradoria-Geral da República. (Relator: Mário Serrano).

Pereira, F. (2016). *El agente infiltrado desde el punto de visa del garantismo procesal penal* (2.ª Ed). Juruá Editorial.

Pereira, R. C. (1996). O consumo e o tráfico de droga na lei portuguesa. *Revista do Ministério Público*(65), pp. 59-76.

Pereira, R. C. (2004). O "agente encoberto" na ordem jurídica portuguesa. In Centro de Estudos Judiciários, *Medidas de combate à criminalidade organizada e económico-financeira* (pp. 11 e ss.). Coimbra Editora.

Pereira, V. (2016). Contributo para o estudo das ações encobertas: Breve resenha histórica. *Revista de Investigação Criminal*(10), pp. 102-120.

Poiares, N. (2019). A cibersegurança à luz da criminologia moderna. In *Revista científica sobre ciberlaw do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa*(VII). https://comum.rcaap.pt/bitstream/10400.26/34692/1/A-CIBERSEGURAN%c3%87A-%c3%80-LUZ-DA-CRIMINOLOGIA-MODERNA.pdf

Pradillo, J. (2013). *Problemas procesales de la ciberdelincuencia.* Editorial Colex.

Quivy, R. & Campenhoudt, L. V. (2008). *Manual de investigação em ciências sociais* (5ª Ed.). Gradiva.

Ramalho, D. S. (2013a). A investigação criminal na dark web. In *Revista da Concorrência e Regulação, 4*(14), pp. 383-429. https://www.concorrencia.pt/sites/default/files/imported-magazines/CR14_15_-_Victor_Castro_Rosa.pdf

Ramalho, D. S. (2013b). O uso de malware como obtenção de prova em processo penal. *Revista da Concorrência e Regulação, 4*(16), pp. 195-243.

https://www.concorrencia.pt/sites/default/files/imported-magazines/CR16_-_David_Silva_Ramalho.pdf

Ramalho, D. S. (2017). *Métodos ocultos de investigação criminal em ambiente digital.* Almedina.

Ramos, A. D. (2017). *A prova digital em processo penal: O correio eletrónico* (2.ª Ed.). Chiado Editora.

Ramos, A. D. (2022). *O agente encoberto digital: Meios especiais e técnicos de investigação criminal.* Almedina.

Resolução da Assembleia da República n.º 88/2009, de 15 de setembro. *Diário da República*. Série I, n.º 179/2009, pp. 6354-6378. Assembleia da República. (Aprova a Convenção sobre o Cibercrime).

Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto. *Diário da República*. Série I, n.º 163/2017, pp. 5035-5037. Presidência do Conselho de Ministros. (Cria o grupo de projeto denominado Conselho Superior de Segurança do Ciberespaço).

Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho. *Diário da República*. Série I, n.º 113/2015, pp. 3738-3742. Presidência do Conselho de Ministros. (Aprova a estratégia nacional de segurança do ciberespaço).

Reunião Plenária de 10 de julho de 2009. *Diário da Assembleia da República*. Série I, n.º 102/2009, pp. 1-71. Assembleia da República.

Reunião Plenária de 21 de junho de 2001. *Diário da Assembleia da República*. Série I, n.º 99/2001, pp. 1-39. Assembleia da República.

Reunião Plenária de 3 de junho de 2022. *Diário da Assembleia da República*. Série I, n.º 21/2022, pp. 1-50. Assembleia da República.

Rodrigues, B. S. (2009). *Direito penal parte especial - Tomo I: Direito penal informático-digital.* Coimbra Editora.

Rodrigues, B. S. (2011a). *Da prova penal: Novos métodos "científicos" de investigação criminal nas fronteiras das nossas crenças.* Rei dos Livros.

Rodrigues, B. S. (2011b). *Da prova penal - Tomo IV: Da prova eletrónico-digital e da criminalidade informático-digital.* Rei dos Livros.

Roxin, C. (2000). *Derecho Procesal Penal.* Editores del Puerto.

Sanchez, J. M. (1995). *La moderna problemática jurídico penal del agente provocador.* Tirant lo Blanch.

Santo, P. E. (2015). *Introdução à metodologia das ciências sociais: Génese, fundamentos e problemas* (2ª Ed.). Edições Sílabo.

Santos, N. R. P. (2020). O auxílio do colaborador de justiça em Portugal: Uma visão jurídico-policial. *Revista da Faculdade de Direito da Universidade de Lisboa, LXI*(2), pp. 507-550. https://comum.rcaap.pt/bitstream/10400.26/35965/1/Santos%20NRP%20%282021%29%20O%20aux%c3%adlio%20do%20colaborador%20de%20justi%c3%a7a%20em%20Portugal%20-%20uma%20vis%c3%a3o%20jur%c3%addico-policial.pdf

Silva, D. S. (2016). Da validade processual penal das provas obtidas em sites de relacionamento e a infiltração de agentes policiais no meio virtual. *Revista Brasileira de Ciências Criminais, 24*(120), pp. 203-235. https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2016;1001128393

Silva, E. A. (2003). *Crime organizado: Procedimento probatório.* Editora Atlas.

Silva, G. M. (1994). Bufos, infiltrados, provocadores e arrependidos: Os princípios democráticos e da lealdade em processo penal. *Revista Direito e Justiça, VIII*(2), pp. 27-34.

Silva, G. M. (2005). Meios processuais expeditos no combate ao crime organizado (a democracia em perigo?). *Revista de Direito da Universidade de Lisboa*(3), pp. 69-81.

Silva, G. M. (2015). *Direito processual penal português: Do procedimento* (Vol. III). Universidade Católica Editora.

Silva, G. M. (2020). *Direito processual penal português: Noções e princípios gerais. Sujeitos processuais. Responsabilidade civil conexa com a criminal. Objeto do processo* (2ª Ed). Universidade Católica Editora.

Sistema de Segurança Interna. (2020). *Relatório Anual de Segurança Interna - 2020.* https://www.portugal.gov.pt/download-

ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3D.

Sistema de Segurança Interna. (2021). *Relatório Anual de Segurança Interna - 2021*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3D.

Sistema de Segurança Interna. (2022). *Relatório Anual de Segurança Interna - 2022*. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

Sousa, P. P. (2010). Ações encobertas: Meio enganoso de prova? Agente Infiltrado e agente provocador: Outras questões. *Revista do Centro de Estudos Judiciários*(14), pp. 231-247.

Teles, I. G. (2000). *Introdução ao estudo do direito* (1ª Ed., Vol. II). Coimbra Editora.

Valente, M. M. G. (2010). *Processo Penal - Tomo I* (3.ª Ed.). Almedina.

Valente, M. M. G. (2019). *Teoria Geral do Direito Policial* (6ª Ed.). Almedina.

Venâncio, P. D. (2011). *Lei do cibercrime: Anotada e comentada.* Coimbra Editora.

Venâncio, P. D. (2023). *Lei do cibercrime: Anotada e comentada - Atualizada pela lei n.º 79/2021, de 24 de novembro.* Editora D'Ideias.

Verdelho, P. (2003). Cibercrime. In Associação Portuguesa de Direito Intelectual (Vol. IV). *Direito da sociedade da informação* (pp. 347-383). Coimbra Editora.

Vilela, A. J. & Pinto, N. T. (2022, 28 de julho). *PJ usou agentes provocadores em caso de tráfico de droga?* Sábado. https://www.sabado.pt/portugal/detalhe/pj-usou-agentes-provocadores-em-caso-de-trafico-de-droga

Zanella, E. L. (2016). *Infiltração de agentes e o combate ao crime organizado: Análise do mecanismo probatório sob o enfoque da eficiência e do garantismo* (2.ª Ed.). Juruá Editorial.