INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

A NATUREZA JURÍDICA DA AÇÃO DO AGENTE INFILTRADO DIGITAL

António José da Silva Catana

Dissertação de mestrado em Ciências Policiais

Área de especialização em Criminologia e investigação Criminal

Orientação científica:

Prof. Doutor Eduardo Vera Cruz Pinto

Lisboa, 2018

Aos meus pais por terem feito

de mim quem hoje sou...

A legitimação dos novos meios de investigação não se faz agora ao ritmo e à medida das novas possibilidades técnicas e como resultado da sua projecção directa sobre o direito.

"o que é tecnicamente possível não é, só por si e sem mais, legítimo"

Manuel da Costa Andrade

AGRADECIMENTOS

Elaborar um trabalho da natureza como é uma dissertação de mestrado não pode ser reconduzindo unicamente ao seu autor. Orbitam na sua feitura instituições e pessoas que em conjunto contribuem significativamente para o sucesso do trabalho. Como tal, quero deixar aqui expresso a minha sincera gratidão.

Começo pelo Instituto de Ciências Policiais e Segurança Interna e de todos que trabalham nele, de ter tido o privilégio de com eles privar.

Ao meu orientador senhor Professor Doutor E. Vera Cruz Pinto que desde a primeira hora acarinhou este projeto e me deu incentivo necessário para o levar a bom porto.

A minha família e a minha companheira Carla Azevedo que comigo trilharam este caminho, suportaram os obstáculos e as dificuldades próprios que um trabalho desta dimensão acarreta.

Uma palavra muito merecida aos meus amigos João e Rodrigo que tiveram a paciência de me escutar e de contribuírem com a própria opinião para enriquecer esta minha dissertação.

O meu grande

Bem Haja

RESUMO

Não temos dúvidas que nos dias de hoje os meios informáticos são já indissociáveis do quotidiano de cada um. A rapidez e, mais propriamente, a facilidade com que se pode comunicar com familiares, amigos, conhecidos ou não, para qualquer parte do globo, atingiu proporções que ainda há poucos anos eram tidas como inimagináveis.

Mas se esta dinâmica tecnológica abriu novas portas ao bem-estar de todos nós, o mundo cibernético não deixou indiferentes os agentes criminosos, potenciando uma nova criminalidade.

Com novos tipos de crime ou simplesmente com recurso a um novo meio, caraterizado pela falta de fronteiras e pelo anonimato, estes vêm pôr à prova o acompanhamento por parte dos investigadores. As novas tecnologias não trazem apenas obstáculos à investigação criminal, também permitem potencializar novos meios de obtenção de prova, ou ainda a adaptação de métodos tradicionais.

É neste contexto que a figura do agente infiltrado digital emerge. Como tal importa saber como se enquadra no ordenamento português. Os meios ocultos de obtenção de prova são um meio excecional de investigação, mas que conflituem com direitos fundamentais. Perante isto, temos de saber qual o resultado da atividade do agente infiltrado face às provas que o tribunal vier a apreciar.

Palavras-Chaves: Agente infiltrado, Prova, Meios de Prova, Ciberespaço, Cibercrime, Comunicações, Dados, Digital.

ABSTRACT

We have no doubt that nowadays computerized means are inseparable from everyone's daily life. The speed and easiness through which is possible to get in touch with relatives or friends to any part of the globe has just reached proportions which would be unimaginable a few years ago.

However, if this technological dynamic opened new doors to the welfare of us all, the cyber world has not left indifferent criminal agents either, fostering a new criminality.

With new types of crime or simply the access to a new mean characterized by being borderless and anonym, the digital era has arrived to test both researchers and security systems. New technologies do not only bring obstacles to criminal investigation; they also create or adapt methods for obtaining evidences.

It is in this context that the figure of the digital undercover agent emerges and falls within the Portuguese legal order. The hidden means of obtaining evidences are exceptional means of investigation which collides with fundamental rights. In this regard, it is important to know what is the result of the activity of the undercover agent in light of the evidences that the court will take into consideration.

Keywords: Undercover agent, Evidence, Means of evidence, Cyberspace, Cybercrime, Communications, Data, Digital.

LISTA DE SIGLAS

Art.º	Artigo
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
DCIAP	Departamento Central de Investigação e Acão Penal
GNR	Guarda Nacional Republicana
OPC	Órgão de Polícia Criminal
PSP	Polícia de Segurança Publica
RASI	Relatório Anual de Segurança Interna
RJAE	Regulamento jurídico das ações encobertas

ÍNDICE

INTRODUÇÃO

As tecnologias têm duas faces: se, por um lado, contribuem para o desenvolvimento económico, social e cultural das sociedades, por outro permitem também o fomento da criminalidade. A Convenção do Cibercrime de 2001 foi o mote que a União Europeia deu para o combate à crescente criminalidade informática, arranjar soluções para lidar com a prova digital e, ainda, regular os meios de obtenção de prova no âmbito digital.

Dos meios de obtenção de prova, cabe-nos destacar a figura do agente infiltrado no meio digital que, partindo da legislação das ações encobertas tradicionais, foi adaptada à realidade do mundo cibernético. Para solucionar lacunas que a nova figura, ou, mais corretamente, esta figura adaptada à nova realidade traz, somos reconduzidos para o regime das escutas. Esta solução merece alguma atenção de forma a avaliar se é esse o caminho mais correto.

Este meio de obtenção de prova é bastante intrusivo dos direitos fundamentais dos cidadãos pois, nos dias de hoje, há uma grande diversidade de informação armazenada nos sistemas informáticos e, através da infiltração, as autoridades judiciárias competentes podem aceder a um conjunto de informação que abarca toda a vida pessoal de um individuo.

Para o processo penal num sentido restrito, a prova é a demonstração inequívoca da realidade material de um facto (existência de um ato jurídico) e num sentido lato, o processo ou conjunto de procedimentos que tem por fim tal demonstração. A produção de prova está sujeita ao princípio do contraditório “pela prova”; isto equivale a dizer que a formação da prova pressupõe que todos os atos probatórios devam ser efetuados através da “participação contemporânea e contraposta das partes” em sede de julgamento. Tal significa que será somente através de atos contraditórios que se poderá efetuar a aquisição da prova. Desta forma, garante-se que todo e qualquer elemento de prova utilizado pelo tribunal na fundamentação da sentença tenha passado por um processo de discussão envolvendo forçosamente o arguido, pois “Não valem

em julgamento, nomeadamente para o efeito de formação da convicção do tribunal, quaisquer provas que não tiverem sido produzidas ou examinadas em audiência" art.º 355.º, n.º 1 do Código de Processo Penal, com a exceção das situações previstas no n.º 2. Se a prova está sujeita a princípios estruturantes, os meios de prova e os meios de obtenção de prova não ficam isentos de se subjugar a outros princípios consagrados na Constituição da República. Os meios de obtenção de prova são instrumentos utilizados pelas Autoridades Judiciárias e, subsequentemente, pelos Órgãos Policiais Criminais cujo intuito da sua aplicação na investigação é a recolha de indícios de prova. Contudo, a obtenção destes meios deve desenvolver-se, impreterivelmente, sob a garantia e prossecução dos direitos fundamentais consagrados na Constituição da República Portuguesa, isto é, não ofender quaisquer direitos pessoais e princípios fundamentais de forma a não se ter uma justiça amoral e enferma.

Balizada a atuação do agente infiltrado, temos ainda limites quanto às proibições de produção de prova que podem ser ainda subdivididas em proibições de temas, meios e métodos. O segredo de Estado é um dos temas que não deve ser investigado art.º 137.º e art.º 187.º do Código Processo Penal, pois aqui, o interesse público existente na salvaguarda do segredo de estado prevalece sobre o interesse, também público, da descoberta da verdade material. Quanto a meios proibidos temos, mesmo que autorizados pelo juiz de instrução, a proibição da produção de prova através de suportes técnicos e respetivas transcrições quando tiverem sido gravadas conversações em que intervenham o Presidente da República, o Presidente da Assembleia da República ou o Primeiro Ministro art.º 11.º, n.º 2, alínea b do Código Processo Penal. Por fim, os métodos de prova são os procedimentos usados para a aquisição de meios de prova, que não podem ofender os direitos, liberdades e garantias plasmados na Constituição da República Portuguesa.

Assim temos métodos absolutamente proibidos, sendo o processo penal direito constitucional aplicado, há princípios basilares como o princípio da dignidade da pessoa humana que não pode ser desrespeitado. Encontramos

este respeito no art.º 32.º, n.º 8 Constituição da República Portuguesa em que é nula toda a prova obtida "… mediante tortura, coação, ofensa da integridade física…". Mas nem sobre todos os direitos constitucionais recai a absoluta proibição, outros há em que é relativamente proibido como a intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações art.º 34.º Constituição da República Portuguesa, a não ser que o visado dê o seu consentimento ou haja autorização judicial. Estes conceitos de métodos absolutamente ou relativamente proibidos são replicados no código processo penal no seu art.º 126.º.

Se o recurso à figura do agente infiltrado e seus meios de obtenção de prova estão bem delimitados num ambiente não digital, fica a questão, e no mundo cibernético?

A lei do cibercrime n.º 109/2009, de 15 de setembro através do seu art.º 19.º reconduz as ações encobertas em ambiente digital a Lei n.º 101/2001, de 25 de agosto, ou seja, rege-se pelo mesmo regime em ambiente não digital, mas o art.º 19.º, n.º 2 é claro que quando "Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações". E aqui começam as dúvidas, é suficiente este regime de analogia?

A nossa proposta, ao abordar a temática da investigação no mundo digital na perspetiva do recurso à figura do agente infiltrado, é a de encontrar uma resposta perante a matéria em causa, se temos suficiência de lei, se o recurso a institutos por analogia é correto, se apenas a prova digital é permitida ou estaremos perante um quadro de atividade que carece de uma legislação autónoma.

ESTADO DA ARTE

O objetivo desta dissertação de mestrado tem como pano de fundo essencialmente clarificar se a legislação sobre o regime jurídico em causa é

deficitária e, ainda, qual o valor jurídico atribuído à investigação oculta pela figura em estudo. Sabido que o direito penal se move em torno de princípios estruturados e que a investigação criminal, na descoberta da verdade material, por vezes tende a colidir com direitos liberdades e garantias, a obtenção de elementos de prova não pode ultrapassar esses limites, para que em sede de julgamento não sejam depois passíveis de serem anulados.

Importa esclarecer quais são os limites legalmente admissíveis quanto ao recurso do agente infiltrado digital: se, por exemplo, qualquer crime pode ser investigado através deste meio, quem são os agentes em causa, se os recursos a programas informáticos também são considerados válidos se os elementos recolhidos têm que ser integralmente digitais.

Muitas questões se levantam a este propósito. Estudos sobre o agente infiltrado estão bastante difundidos, e este pode ser o ponto de partida para comparar se as características são similares no mundo do digital. Assim como a prova, já muitos autores se pronunciaram sobre qual a sua finalidade no processo penal, e recentemente o termo “prova digital” começa a emergir na literatura jurídica.

Em suma, o tema que nos propomos investigar ainda não é corrente no meio académico: ele está parcialmente estudado, ou seja, facilmente encontramos obras que abordem o tema de prova digital e outras do agente infiltrado, mas a comunhão das duas em ambiente digital ainda não. Acreditamos que este é o contributo válido da nossa dissertação: reunir dois mundos, o jurídico e o informático, sob a mesma capa.

METODOLOGIA DE INVESTIGAÇÃO

É frequente e natural associar a trabalhos de investigação, como é uma dissertação de mestrado, que a hipótese proposta a estudo tenha como ponto de partida uma questão. Não somos alheios a este método, e como tal focamos

a atenção no próprio título da nossa dissertação que servirá de guia no nosso labor.

No decorrer do presente trabalho desenvolveremos uma metodologia essencialmente teórica, sobretudo descritiva, porquanto implicará "estudar, compreender e explicar a situação atual do objeto de investigação",[1] neste caso em concreto o "Agente infiltrado digital".

Num primeiro Capítulo vamos realizar um enquadramento geral sobre a figura do agente infiltrado em que partimos da génese da figura de infiltração em termos gerais. Segue-se a distinção do agente infiltrado com outras figuras que se tocam e que muitas vezes acabam por se confundir, dai ser também importante fazer uma breve introdução sobre essas outras figuras jurídicas que estão muito perto do agente infiltrado. O ponto seguinte, ainda dentro do primeiro capítulo, é o de identificar quais os pressupostos do recurso do infiltrado assim como os tipos de ações encobertas que podem ser alvo através do nosso método oculto de investigação. Para terminar, analisaremos outros ordenamentos jurídicos e formaremos uma opinião sobre quem é o terceiro no regime jurídico das ações encobertas.

No segundo capítulo, vamos entrar mais precisamente no mundo digital, saber que sociedade é esta e conhecer o espaço em que se move. Vamo-nos socorrer da legislação tanto do nosso ordenamento como de outros que contemplam a figura do agente em ambiente digital. Também aqui será abordado a problemática de possíveis figuras que são confundidas com a figura do agente infiltrado. Por fim, será aborda o tema da prova digital e os pressupostos do agente infiltrado em ambiente digital.

---

[1] CARMO, Hermano, FERREIRA, Manuela Malheiro, *Metologia da Investigação*, Guia para Auto-aprendizagem, Lisboa, Universidade Aberta, 1998, p213

Terminamos com um terceiro capítulo que tem o seu foco nas entrevistas realizadas a diferentes entidades, as quais permitem complementar o nosso trabalho através do qual pretendemos saber como se relaciona o mundo do cibercrime com o da cibersegurança e o da ciberdefesa.

1 CAPÍTULO I - O AGENTE INFILTRADO NO MUNDO FÍSICO

1.1 GÉNESE DA FIGURA DA INFILTRAÇÃO

Se há evidências inquestionáveis, por estarem bem documentadas, é que, ao longo da história, várias foram as civilizações que entraram em conflito umas com as outras. Tais confrontos no campo de batalha ficaram a dever-se às mais diversas causas, como por exemplo questões que envolviam a defesa do seu território ou simplesmente relacionadas com a sobrevivência da própria comunidade. Assim, tendo presente que estamos nos primórdios da civilização, ou seja, um período mais ou menos distante, a questão sobre a recolha de informações dos adversários colocava-se por ser somente no decurso do conflito que esta era adquirida, tendo essencialmente como objetivo, inviabilizar qualquer plano de ataque por parte do inimigo. Com a evolução das comunidades, o papel atribuído às informações sobre os adversários também sofreu um aperfeiçoamento e, nesta matéria, um meio de colmatar a falha que resultava em escassos conhecimentos sobre os rivais passou pela aquisição da informação de uma forma prévia. Esta mudança vai permitir que sejam definidas estratégias por parte dos decisores envolvidos nos conflitos, apenas pelo facto de estarem na posse de conhecimentos recolhidos com antecedência. Uma das táticas utilizadas para a recolha de informações sobre as atividades que poderiam afetar a segurança da comunidade, que inicialmente tem apenas enfoque nos vizinhos foi, sem margem para dúvida, feita de uma forma o mais dissimilada possível, podendo reconduzir este comportamento facilmente à arte de “Espiar", que significa “Observar em segredo, com o objetivo de conseguir informações”.[2]

Não é de estranhar que a figura do espião seja tão velha como a história da humanidade. Na zona que hoje é designada por Turquia, os hititas que habitaram a região há mais de 3 mil anos, já circulavam informações sobre os

[2] Dicionário infopedia; https://www.infopedia.pt/dicionarios/lingua-portuguesa/espiar

inimigos, escrita em pedaços de argila, o que revela bem de quão longe vem a espionagem.[3] No “Antigo Testamento”, também temos referências a esta figura, quando Moisés enviou à terra de Canaã, em missão, doze espiões para descobrir quem morava lá, quão fortes seriam, e também para saber se o solo seria bom para a lavoura. O Rei Alfredo o Grande, (Primeiro rei de Wessex que se auto proclamou rei de Inglaterra) sempre atento à ameaça dinamarquesa, e com o intuito de avaliar a força inimiga utilizou o recurso à infiltração. Foi ele próprio disfarçado de trovador, ao acampamento dos dinamarqueses para conhecer *in loco* o seu inimigo. Tentar saber o que se passava nos reinos vizinhos era uma preocupação dos Reis e, principalmente com aqueles que tinham tronos frágeis, o recurso ao “Espião” era vulgar, com o intuito, porém, de privilegiar a segurança interna, mais do que propriamente para adquirir informações externas com vista a utilizar em futuras relações diplomáticas.

A importância da recolha de informações vitais pode ser aferida pelo secretismo que envolve a espionagem, pois saber-se, qual o número de espiões ao serviço dos governantes não é um dado de fácil obtenção. Afirma-se que Akbar, o grande governador mongol da Índia no Sec. XVI, empregava mais de quatro mil agentes para este fim, e o autodenominado mestre da espionagem prussiana, Wilhelm Stieber sob as ordens de Frederico IV, teve a seu cargo mais de quarenta mil agentes afetos à atividade da espionagem.[4]

Os embaixadores são outra figura sobre a qual recaem suspeitas de terem sido usados como espiões nas relações internacionais, tendo a seu cargo não apenas a tarefa de recolher informações sobre os Estados onde eram colocados, mas também a de fazer propaganda do seu país. Porém, se os espiões

---

[3] KNIGHTLEY, Phillip, *Espiões e espionagem: História da segunda mais velha profissão do mundo,* tradução de MACHADO, Maria José Bellino, Círculo de Leitores, agosto 1990, p19

[4] KNIGHTLEY, Phillip, *Espiões e espionagem: História da segunda mais velha profissão do mundo,* tradução de MACHADO, Maria José Bellino, Círculo de Leitores, agosto 1990, p19

floresciam em tempos de guerra, em tempo de paz definhavam. Assim, não é de estranhar que a espionagem, nesta época, atuava de uma forma amadora, pouca organizada e com meras pretensões ao nível militar, de proteção interna dos estados.

É no Séc. XVI, que o principal conselheiro Sir Francis Walsingham faz, ao serviço da rainha Isabel I, emergir uma espécie de serviço permanente de espionagem, cuja principal atividade seria a de vigiar os jesuítas. Porém, longe ainda do profissionalismo, já que a iniciativa que Sir Francis Walsingham teve foi a de mandar espiões ao estrangeiro para obter informações sobre a Armada Espanhola, uma atitude particular que o próprio financiou.

Contudo, é apenas na Grã-Bretanha, já no início do Sec. XX, que surge na verdadeira aceção da palavra, um serviço de informações, designado por S.I.S. (Secret Intelligence Service) constituindo-se como um departamento governamental e financiado por fundos públicos, cujos funcionários eram predominantemente civis. O objetivo destes serviços era o de roubar segredos a outros países e proteger os seus próprios, tendo autoridade para se manterem operacionais tanto em tempo de guerra como de paz. Estes serviços, que eram o sonho de qualquer burocrata, foram proliferando por todo o mundo, até os mais pobres governos do terceiro mundo não se sentissem Estados soberanos se não possuíssem um serviço de informações.[5]

Michael J. Barrett, conselheiro geral Assistente da CIA, escrevia no Journal of defense and diplomacy, em fevereiro de 1984 que "*a espionagem é a segunda mais antiga profissão, e tão honrosa como a primeira*". Podemos aferir pelas palavras do conselheiro que desde os primórdios da história da humanidade se recorre à recolha de "informações".[6] É com naturalidade que

[5] KNIGHTLEY, Phillip, *Espiões e espionagem: História da segunda mais velha profissão do mundo,* tradução de MACHADO, Maria José Bellino, Círculo de Leitores, agosto 1990, p19

[6] *Ibidem*, p20

constatamos que a espionagem tenha evoluído de um modo amador para profissional, de militar a policial, de acessório em tempo de guerra para se fixar de forma permanente, na qual os Estados nunca afirmam ter serviços secretos, mas sim serviços de recolha de informações, não só sobre os seus inimigos, mas também sobre os seus aliados – o caso Snowden, recentemente vindo a público, é prova viva desta afirmação.

Até ao momento, analisámos uma evolução do recurso à infiltração em que o objetivo é a defesa da comunidade, culminando em ações encobertas de cariz político.[7] Porém, para termos uma visão de âmbito mais policial, temos de recuar ao "Ancien Regime", na França do Séc. XVII.

Em 1667, em virtude da crescente onda de criminalidade em Paris, é criado o "Lugar-tenente de polícia", na regência do Rei Sol durante o período absolutista francês. Mas como era dispendioso, foram criados outros agentes para o coadjuvar "Comissários", e estes por sua vez eram apoiados por inspetores que inicialmente apenas eram chamados quando necessários.[8] Só em 1740, fruto de uma restruturação segundo a qual a carreira de inspetor passa a ser permanente, é que lhes são atribuídas as funções de vigilância e investigação. Com as múltiplas diligências que lhes são atribuídas, passam a ser auxiliados por um "Agent provocateur". A polícia optou por distingui-los entre «aqueles que trabalhavam encobertos, clandestinamente, a que chama eufemisticamente de "*observateurs"*, e aqueles que eram contratados abertamente, que eram comumente conhecidos como *mouches, "sous-inspecteurs",* "*commis"* ou "*préposés".*[9]

[7] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, p19

[8] WILLIAMS, Alan, *The police of Paris, apud* MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal,* Coimbra, Almedina, 1999, p19

[9] *Ibidem*, p20

De entre os contratados, encontramos facilmente reclusos que negoceiam a sua liberdade a troco de uma cooperação com as autoridades, infiltrando-se em locais "perigosos", ou caso fossem de níveis sociais mais elevados seriam encaminhados para um "millieu" diferente, conforme decisão do inspetor. Aos *"sous-inspecteurs"* cabia-lhes em sorte infiltrarem-se com o fim de *seguir, escutar, informar, de provocar e prender os malfeitores sob vigilância.* Como facilmente podemos observar, é possível diferenciar diversas formas de agente, tais como o agente infiltrado, o agente provocador e o agente informador.[10]

Com a revolução francesa, a atividade da polícia parisiense não esmorece e até aumenta os "espions de police" desta vez com os presos, mas que se mantêm encarcerados, são denominados por "moutons de police". Estes agentes passam a ser utilizados para que o governo se possa libertar de sujeitos incómodos contra os quais não há provas para os condenar.[11]Estes novos agentes estão incumbidos de denunciar o pessoal de segurança da prisão ou instigam os companheiros de cela para, logo de seguida, os denunciar. Uma vez mais estamos aqui perante ações de cariz político já que os alvos principais seriam os cidadãos contrários à orientação política geral.[12]

Os serviços destes agentes informadores não ficaram, porém, apenas ligados aos regimes políticos. Em Espanha, a doutrina deu pouca relevância a esta figura, mas a igreja, no período da inquisição, recorreu sistematicamente aos agentes em causa. Em Inglaterra, para fazer face a uma ausência de uma força policial e a um aumento da taxa de criminalidade, o parlamento concedia prémios e imunidades a quem fornecesse provas incriminadoras, sendo esta uma forma de levar a sociedade a participar na supressão do crime. Contudo, a

---

[10] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, p22

[11] COOB, *Polizia e popolo. La protesta popolare in Francia, apud,* MEIREIS, *opcit,* p21

[12] DELL'ANDRO, *Agente provocator, Apud,* Meires Manuel Augusto Alves, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal,* Coimbra, Almedina, 1999, p22

partir de 1816, com o "Bennet's Act" o sistema de recompensas é transferido do parlamento para os tribunais. Por cá, a figura do provocador aparece na literatura em 1906 ligada também ao regime político, e é descrita como corrupta e monstruosa, através da qual os agentes acusam inocentes para conspirações que eles próprios criam.[13]

1.2 A LEI E O AGENTE INFILTRADO EM PORTUGAL

Em Portugal, a primeira abordagem legislativa feita à figura do agente infiltrado surge no decreto-lei nº430/83, de 13 de dezembro (Regime jurídico do tráfico e consumo de estupefacientes).

É no artigo 52.º *(Conduta não punível)* do referido diploma que encontramos os limites impostos à conduta do agente, delimitando a prevenção e investigação, inibindo qualquer ato de instigação, podendo apenas exercer atos de aceitação de estupefacientes como podemos constatar da leitura do seu *n.º 1 "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 terceiro a entrega de estupefacientes ou substâncias psicotrópicas". N.º 2 "O relato de tais factos será junto ao processo no prazo máximo de 24 horas".* Este diploma manteve-se em vigor até ser revogado pelo decreto-lei n.º 15/93, de 22 janeiro, tendo a epígrafe (conduta não punível) e conteúdo do artigo 52.º do anterior decreto-lei sido transcrita na íntegra para o artigo 59.º do novo diploma.

A lei seguinte, que passou a contar com a possibilidade do recurso da figura do agente infiltrado, foi a lei n.º 36/94, de 29 de setembro sobre as medidas de combate à corrupção e criminalidade económica e financeira, em que fica patente a possibilidade de recurso ao agente infiltrado para efeitos preventivos. Este diploma veio alargar o leque de crimes em termos de prevenção e

[13] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, p26

investigação criminal, tendo, porém, em atenção, o facto de que agora os atos carecem de prévia autorização judiciária, como decorre do n.º 2 do artigo 6.º, que abaixo transcrevemos:

Artigo 6.º *(Atos de colaboração ou instrumentais) n.º 1 É legítima, com vista à obtenção de provas em fase de inquérito, a prática de atos de colaboração ou instrumentais relativamente aos crimes previstos no n.º 1 do artigo 1.º do presente diploma. N.º 2 Os atos referidos no número anterior dependem sempre da prévia autorização da autoridade judiciária competente.*

Porém, a alteração mais significativa viria a ocorrer com a lei 45/96, de 3 setembro, em que o artigo 59.º do decreto-lei 15/93 foi substancialmente modificado e, ainda, com o aditar de um novo preceito, o artigo 59.º - A *Proteção de funcionário e de terceiro infiltrados*, em que, pela primeira vez aparece explicitamente referido o termo “infiltrado”.

Esta nova Lei veio estabelecer importantes alterações, como, por exemplo, o facto de, para além do funcionário de investigação, possa ser admitido um terceiro que atue sob controlo da Polícia Judiciária. Em termos de atividade que pode desenvolver, para além de aceitar também pode deter, guardar, transportar e entregar estupefacientes. No que toca a prévia autorização judiciária, esta, nas situações de urgência, pode ser validada no dia seguinte. O prazo da apresentação do relato foi alargado de 24 para 48 horas e será apenso ao processo se for imprescindível para efeitos de prova. Determinou-se ainda a restrição da livre assistência ou a exclusão da publicidade da audiência caso o agente infiltrado comparecesse.

O regime jurídico das ações encobertas para fins de prevenção e investigação criminal (RJAE) em vigor é hoje o diploma que consagra a figura do agente infiltrado, precisamente na lei 101/2001, de 25 de agosto. O recurso à figura de agente infiltrado perdeu a exclusividade no caso dos crimes de tráfico de droga e combate à criminalidade económica e financeira, como se constata no seu artigo 2.º. Mesmo que o seu campo de ação encoberta tenha sido

alargado a novos crimes graves, o recurso ao agente infiltrado, mas não deixou por isso de fora quais as suas finalidades, prevenção e investigação, e o seu correto entendimento permitindo compatibilizar o regime com o n.º 8 do artigo 32.º da Constituição e com o n.º 1 e n.º 2 do artigo 126.º do código processo penal.[14]

O artigo 1.º define o objeto das ações encobertas, tendo como fim a prevenção e repressão criminal, e no que diz respeito a quem pode ser um agente infiltrado o presente diploma não fez alterações nessa matéria, em relação ao que estava em vigor, continuando reservado à Polícia Judiciária ou a terceiros atuando sob controlo daquela polícia. Não nos choca que as ações sejam, para além de prevenção, um recurso para a repressão, mas desde que se encontrem salvaguardados os direitos liberdades e garantias. Quanto ao terceiro como particulares, estando previsto que seja utilizado, temos dificuldade em aceitar como agente infiltrado, seguindo aqui Guedes Valente[15], que diz, nem que seja pela dificuldade de um controlo eficaz da conduta do particular.

Temos de acrescentar que podem ainda ser agente infiltrados, agentes de outros Estados, conforme nos mostra o artigo 160.º-B da lei 104/2001 lei da cooperação judiciária internacional em matéria penal, desde que tenham idêntico estatuto aos funcionários de investigação criminal portugueses, que exista tratado ou convenção internacional, cabendo ao juiz do tribunal central de instrução criminal competente a competência para proceder a tal autorização judicial.

---

[14] PEREIRA, Rui, "O "agente encoberto" na ordem jurídica portuguesa", *in Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa,* Vol. II, Coimbra Editora, 2005, p296

[15] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014, p515

Artigo 160.º-B Acções encobertas

1 - Os funcionários de investigação criminal de outros Estados podem desenvolver acções encobertas em Portugal, com estatuto idêntico ao dos funcionários de investigação criminal portugueses e nos demais termos da legislação aplicável.

2 - A actuação referida no número anterior depende de pedido baseado em acordo, tratado ou convenção internacional e da observância do princípio da reciprocidade.
3 - A autoridade judicial competente para a autorização é o juiz do Tribunal Central de Instrução Criminal, sob proposta do magistrado do Ministério Público junto do Departamento Central de Investigação e Acção Penal (DCIAP).

No artigo 2.º, relativo ao âmbito de aplicação, estão aí elencados de forma taxativa os crimes em relação aos quais são admissíveis as ações encobertas. Convém alertar que este diploma não revogou a lei 36/94; assim, temos ainda alguns crimes para além dos elencados na lei 101/2001, em relação aos quais é admissível o recurso a agentes infiltrados, como é o caso da alínea b) do artigo 1.º "administração danosa do sector publico" que não encontramos na nova Lei das Ações Encobertas. Dizer também que o recurso a ações encobertas que vá para além dos crimes referenciados no diploma, vai gerar uma prova proibida.

Para além do catálogo de crimes enunciados no artigo 2.º do (RJAE), vem logo de seguida o artigo 3.º lembrar que não é por se estar perante um crime identificado no RJAE que se justifica uma ação infiltrada. É exigido também que a ação seja adequada aos fins de prevenção e repressão criminais e, mais ainda, que seja proporcional, quer às finalidades supracitadas bem como quer às do crime sob investigação. Podemos afirmar que, caso se investigue um crime de tráfico de droga em que se conclua estarmos perante um consumidor esporádico, seria aqui desproporcional recorrer a uma operação encoberta. Daí ser exigida uma devida ponderação dos meios antes da sua utilização. Neste artigo, temos a alínea n.º 2 "não obrigação de participação em ação encoberta",

ou seja, têm que os agentes ser exclusivamente voluntários. Aqui, acreditamos que a preocupação é a de que quando se recruta um agente ele tenha livre decisão, já que ele vai se envolver em atividades ilícitas e com situações que podem ter risco para a sua vida.

Segue, no n.º 3 do presente artigo, que em fase de inquérito a autorização judicial é da competência do Ministério Público e que, caso não haja despacho de recusa nas setenta e duas horas seguintes, esta se considera validada. Ora, perante situações em que sejam postos em causa direitos fundamentais, acreditamos que, seja em fase de inquérito, seja de prevenção criminal, que um deferimento tácito não é adequado.

Os artigos seguintes, 4.º e 5.º respetivamente, têm subjacente a proteção do agente infiltrado a dois níveis. A primeira preocupação é a de garantir a proteção do funcionário e terceiro, comum à proibição de junção do relato, a não ser que tal seja absolutamente indispensável em termos probatórios n.º 1 do artigo 4.º; caso o juiz entenda que seja necessário a presença do agente em tribunal, terá que ser aplicado o n.º 1 do artigo 87 do código processo penal assim como a lei 93/99, lei de proteção de testemunhas. A segunda preocupação é a possibilidade do uso de uma identidade fictícia artigo 5.º. exclusiva de agente de polícia criminal e não sendo atribuída ao terceiro se for um particular. O ponto de maior relevância em termos de processo é se devemos considerar apenas o relato do agente para que o tribunal se possa pronunciar, e levar a que o arguido seja condenado ou não. Pensamos que aqui devem ser tidos em conta outros meios complementares para comprovar o relato do agente, como fotografias e outros documentos e, se possível, outras testemunhas.

A isenção da responsabilidade de determinados atos, como atos preparatórios ou de execução de uma infração de comparticipação ou autoria mediata vem consagrado no artigo 6.º. Aqui, temos os limites pelos quais o agente tem de pautar a sua conduta no decorrer da ação encoberta, ficando isento de responsabilidade criminal; ou seja, estamos perante uma causa de exclusão de ilicitude. A nossa preocupação sobre a desresponsabilização do

agente vai mais longe quando pensamos em atos que tenham de ser praticados para que determinada organização permita a entrada nelas, como são vulgarmente conhecidos atos de iniciação que, neste caso, podem muito bem ser ilícitos. Fica o agente protegido pelo artigo 35.º do código penal, “estado de necessidade desculpante” ou a situação também deveria estar enquadrada na isenção de responsabilidade do artigo 6.º da RJAE.

Para concluir, em termos legislativos sobre o agente infiltrado temos ainda a lei 109/2009, de 15 de setembro, lei do Cibercrime, sendo esta última a que mais relevância tem para a nossa dissertação.

Com este diploma, o leque de ação do agente infiltrado volta a ser alargado a crimes específicos como danos relativos a programas informáticos, a sabotagem informática, acesso ilegítimo, interceção ilegítima, reprodução ilegítima de programa protegido e, através do artigo 19.º, aos crimes previstos na lei 101/2001, de 25 de agosto e aos cometidos por meio de um sistema informático quando a pena máxima for superior a cinco anos.

Finalmente, um ponto de grande relevo que cumpre mencionar está relacionado com a cooperação internacional, tendo em conta as características próprias, em termos de territorialidade, em que o cibercrime se move. Este diploma, por força do artigo 19.º, implica que a lei 101/2001, de 25 de agosto esteja também presente, obrigando a uma aplicação em conjunto dos dois diplomas quando esteja em causa o recurso à figura do agente infiltrado com meios informáticos. Como temos uma conjugação de ambas as leis, os princípios invocados na lei 101/2001 também se mantêm para a lei 109/2009.

Como podemos observar, o nosso legislador optou por regulamentar a figura do agente infiltrado em diploma próprio, não a incluindo, portanto, num código. Podemos assim concluir que a maior preocupação deste meio de obtenção de provas seja o de o considerar como uma técnica de investigação

excecional[16], estando, portanto, rodeado de fortes medidas relativamente ao seu recurso, pelo facto de poder atingir, de forma violenta, direitos fundamentais.

1.3 MÉTODOS OCULTOS DE INVESTIGAÇÃO

Não podíamos abordar o nosso estudo sobre o agente infiltrado sem antes fazer uma abordagem de forma generalista sobre quais os métodos ocultos ao dispor da investigação consagrados no nosso ordenamento. Com estes meios, o que se pretende alcançar é a verdade material dos factos ocorridos, sustentada pela obtenção de prova, seja através de intromissões nas telecomunicações, agentes infiltrados, homens de confiança, observação oculta, videovigilância, buscas on-line, gravação de imagem ou palavras com câmara e microfones ocultos. A celeuma que se gera em volta deste tema de métodos ocultos é evidente e facilmente entendida nas palavras de Costa Andrade[17], o qual afirma ser uma intromissão nos processos e ação das pessoas concretamente visadas, e, como tal uma ingerência na liberdade das pessoas, visando, em contrapartida, justificar um ambiente de maior segurança para todos os cidadãos.

No nosso ordenamento jurídico, não temos elencados num código todos os métodos ocultos de investigação passíveis de ser utilizados para efeitos de prevenção e repressão criminal. Acreditamos que teria sido positivo que o nosso legislador assim o tivesse feito, principalmente para efeitos da aplicação do princípio de subsidiariedade; porém, em vez de adotar tal método, fê-lo através de leis avulsas. Temos, como exemplo, a lei n.º 33/2010 para os meios técnicos de controlo a distância ou a lei 101/2001 ações encobertas. Caso existisse uma ordenação dos métodos ocultos de investigação, quando fosse solicitado um determinado meio, o juiz podia recusar ou não em virtude de um outro meio menos gravoso ainda não ter sido utilizado. Sobre a questão se devem os

[16] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014, p491

[17] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, A reforma do código de processo penal*, Coimbra Editora, 2009, p105

métodos ocultos de investigação ser ou não vertidos em código, exceção feita atualmente às escutas telefónicas artigo 187.º e seguintes do código processo penal, somos da opinião que sim, excluindo apenas de tal circunstância o regime das ações encobertas, que acreditamos deva estar regulado em lei especial que lhe dê outro rigor e cuidado quanto ao seu recurso.

Para podermos ficar com uma perceção que os métodos ocultos de investigação podem ser graduados, basta verificar que no artigo 188.º CPP qualquer órgão de polícia criminal pode efetuar as interpretações e a gravação das escutas telefónicas e, no artigo 187.º CPP, estão elencados os crimes que podem ser sujeitos a escutas. Na lei 101/2001 e na lei 109/2009 o leque de crimes que podem ser sujeitos a investigação é menor; ora acreditamos que por estes pontos é possível verificar que há uma grande diferença relativamente aos crimes que são investigados pelo recurso ao agente infiltrado.

Outro ponto que observamos e que é ilustrativo de tal diferença é o seguinte: enquanto o agente infiltrado pode estar em contacto 24 horas com o suspeito, lesando, dessa forma, os seus direitos fundamentais; já as escutas telefónicas, que também lesam esses mesmos direitos, ficam limitadas às conversas que o suspeito efetuar, o que não deixa de invadir a reserva da intimidade da vida privada, à palavra, n.º 1 artigo 26.º CRP, a sua honra, e da inviolabilidade das telecomunicações dos visados n.º 1 artigo 34.º CRP, mas com uma intensidade menor comparada a intensidade das ações encobertas.

Seja qual for o meio oculto de investigação criminal, ele tem de respeitar princípios que recaem também para as ações encobertas, como o princípio da proporcionalidade, da adequação, da necessidade. Daí, a importância do princípio da subsidiariedade, que estabelece que havendo outro meio menos intrusivo será por esse que se deve optar em detrimento de outro mais violador dos direitos fundamentais; por outras palavras, que a diligência a efetuar seja indispensável e adequada para a descoberta da verdade, e só quando a prova é impossível ou muito difícil de obter" n.º 1 artigo 187.º CPP, por meios não lesivos, se opte pelo recurso a métodos ocultos.

Se consultarmos o relatório anual de segurança interna (RASI 2016), verificamos que a criminalidade geral tem vindo a baixar assim como a criminalidade violenta. Porém, crimes envolvendo droga ou crimes informáticos têm evoluído em sentido contrário em relação ao geral. Sendo assim, é de crer que os métodos ocultos de investigação não vão desaparecer. Agora, temos de pensar, como afirma Costa Andrade, que estes meios lesam direitos constitucionalmente consagrados dos elementos sob investigação, sem conhecimento e impossibilidade de reação, como a "privacidade/intimidade, palavra, imagem, inviolabilidade do domicílio.[18] E continua dizendo que pelo recurso aos meios ocultos podem sacrificar-se o direito a recusar testemunho ou depoimento, *o princípio nenotenetur se ipsumacusare, o direito ao silêncio*, culminando na possível contribuição do investigado na sua própria condenação.

1.4 AGENTE INFILTRADO E OUTRAS FIGURAS

Encontramos nas palavas de Benjamim Silva Rodrigues e Manuel da Costa Andrade que as ações encobertas podem ser realizadas por "*Homens de confiança".* Estes autores, ao terem um entendimento bastante extensivo deste conceito, consideram que possam aqui ser incluídas diversas figuras que se aproximam da figura do agente infiltrado. Silva Rodrigues associa ao conceito referido "*Untergrundfahnder, under cover agent, agentes encobertos, agentes infiltrados, Polizeispitzel, detection, polizeiliche Lockspitzel, agent provocateur entrapment".*[19] Diferentemente, Manuel da Costa Andrade considera que podem ser agentes provocadores ou agentes infiltrados "todas as testemunhas que colaboram com as instâncias formais da perseguição penal, tendo, em contrapartida, a promessa da confidencialidade da sua identidade e atividade. Tanto o podem ser os particulares (pertencentes ou não ao submundo da

[18] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, A reforma do código de processo penal*, Coimbra Editora, 2009, p107

[19] RODRIGUES, Benjamim da Silva, *Da Prova Penal, Novos Métodos "Científicos" de Investigação Criminal nas Fronteiras das nossas Crenças,* Tomo IV, 1ed., Reis dos Livros, 2011, p389

criminalidade) como os agentes das instâncias formais, nomeadamente da polícia".[20]

Na jurisprudência, o acórdão do STJ com o n.º de processo 127/10.0JABRG de 27 de junho de 2012, pronuncia-se neste sentido e separa a figura do agente provocador das do agente infiltrado e encoberto, reconduzindo estas duas últimas a uma mesma figura. É precisamente isso que nos mostra os pontos seguintes do acórdão supracitado:

"*XXI - 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 do 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."*

"XXII - O recurso à figura do agente encoberto é legalmente possível desde que feito dentro dos limites fixados pela Lei 101/2001, de 25-08. Já o recurso à figura do agente provocador é veementemente rejeitado quer pela doutrina, quer pela jurisprudência, por constituir um meio enganoso de obtenção de prova alínea a), n.º 2, do artigo 126 do código de processo penal."

1.5 AGENTE PROVOCADOR

Manuel da Costa Andrade, para além de considerar que todas as testemunhas podem ser agentes encobertos, refere ainda que o agente provocador é aquele que de alguma forma precipita o crime "instigando-o,

[20] ANDRADE, Manuel da Costa, Sobre as Proibições de Prova em Processo Penal, Coimbra Editora, 1992, p220

induzindo-o, nomeadamente, aparecendo como comprador ou fornecedor de bens ou serviços ilícitos".[21]

O enfoque do nosso trabalho é sobre o agente infiltrado, mas, como podemos deduzir pelas palavras de Manuel da Costa Andrade, quando se aborda o tema "ações encobertas", não podemos deixar de fazer referência a duas outras figuras que a doutrina traz à colação, que são o agente provocador e o agente encoberto.

Comecemos então pela figura do agente provocador sobre a qual a doutrina é mais consensual.

Como sabemos, o resultado que se pretende alcançar através das ações encobertas, quer sejam elas usadas para fins de cariz político ou puramente judiciais, é o de reunir informações e provas no âmbito da investigação criminal. A obtenção de provas não pode, porém, ser conseguida a qualquer custo pois, caso contrário, temos que a verdade material apurada reconduzir-se-á a regimes típicos de sistemas inquisitórios, nos quais os acusados ou quem fosse afetado pelas decisões jurisdicionais, não têm a oportunidade de se pronunciar sobre a busca e recolha de prova.[22]

Germano Marques da Silva entende, por seu turno, que "a provocação não é apenas *informativa*, mas sobretudo formativa, não revela o crime e o criminoso, mas cria o próprio crime e o próprio criminoso e, por isso, é contrária à própria finalidade da investigação, uma vez que gera o seu próprio objeto".[23]

---

[21] ANDRADE, Manuel da Costa, *Sobre as proibições de Prova em processo Penal*, Coimbra: Coimbra Editora, 1992, p220

[22] MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal,* Coimbra, Almedina, 1999, p195

[23] SILVA, Germano Marques da, *Bufos, Infiltrados, Provocadores e Arrependidos*, in Direito e Justiça, F.D.U. Católica, Vol. VIII, T. 2, 1994, p29.

Já Manuel A. Alves Meireis define como agente provocador "aquele que, sendo um cidadão particular ou entidade policial, convence outrem à prática de um crime, não querendo o crime a *se*, e sim, pretendendo submeter esse outrem a um processo penal e, em último caso, a uma pena". O autor aponta que a questão aqui não se centra em quem leva a cabo a provocação, mas sim na vontade de quem pratica (*animus*) outrem à realização do crime.[24]

Fernando Gonçalves, M. João Alves e Guedes Valente vão na mesma linha de Meireis, mas referem que o "agente provocador pretende submeter outrem a um processo penal e, em última instância, a uma pena, atuando consequentemente com vontade e intenção de, através do seu comportamento, determinar outra pessoa à prática do crime, mas acrescentam que age com dolo ao determinar outra pessoa à prática de um crime, e também, com dolo relativamente à realização do crime".[25]

O professor Rui Pereira faz também a distinção entre agente encoberto e o agente provocador, mas admite o recurso a este último. Não o admite para todas e quaisquer circunstâncias, mas apenas para "crimes graves e em situações de elevada fungibilidade e desde que o crime não acarrete a efetiva lesão de bens jurídicos". Para crimes bagatelares (consumo de droga) o problema já não se coloca na proibição de prova, mas sim de impunibilidade.[26]

O agente provocador não procura recolher provas existentes sobre um crime, pelo contrário induz o instigado, esteja ele ligado ou não a atividades criminosas, na criação de provas ou de numa conduta para conseguir uma

---

[24] MEIREIS, Manuel Augusto Alves, O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal, Coimbra, Editora Livraria Almedina, 1999, p155

[25] GONÇALVES, Fernando, ALVES, Manuel João, VALENTE, Manuel Monteiro Guedes, *Lei e Crime, O Agente Infiltrado vs o Agente Provocador, Os Princípios do Processo Penal*, Coimbra, Almedina, 2001, p256

[26] Pereira, Rui, *O Consumo e o Tráfico de Droga na Lei Penal Portuguesa,* In Revista do Ministério Público, n.º 65, *apud*, ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p36

acusação. Aqui fica patente que a verdade material não é um valor supremo e a busca da mesma não pode ser levada a cabo através de meios criminosos.

A figura do agente provocador não esta regulamentada e não carece de tal necessidade para que seja ilícito o seu comportamento em qualquer investigação criminal. Conforme a Constituição da República consagra no seu n.º 8 do artigo 32.º, 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" e conjugando com o artigo 125.º do CPP , só "são admissíveis as provas que não forem proibidas por lei" e ainda alínea *a)* do n.º 2 do art.º 126.º do CPP diz-nos que não são admissíveis as provas obtidas mediante "a) Perturbação da liberdade de vontade (…) ou utilização de meios cruéis ou enganosos".

A jurisprudência já se pronunciou sobre o agente provocador e não aceita tal figura como podemos comprovar no acórdão processo n.º 182/09. 6JELSB.L1-5 de 23 de novembro de 2011 do tribunal da relação de Lisboa, em que transcrevemos o ponto III:

"IIIº O agente provocador será o membro do órgão de polícia criminal ou alguém a seu mando que pela sua actuação enganosa sugere eficazmente ao autor a vontade de praticar o crime que antes não tinha representado e o leva a praticá-lo, quando sem essa intervenção a actividade delituosa não teria ocorrido. A vontade de delinquir surge ou é reforçada no autor, não por sua própria e livre decisão, mas como consequência da actividade de outra pessoa, o membro do órgão policial;"

O nosso entendimento de agente provocador, tendo em conta o que estudámos e deixámos em cima exposto é o de que este tanto pode ser um agente policial como um particular controlado por aquela polícia. O agente com objetivo de obter provas contra o incitado ou levá-lo a que seja sujeito a um processo penal, incorre numa conduta dolosa. No entanto, o agente provocador não pretende a consumação do delito pois quando o sujeito estiver para cometer

o crime o agente provocador deverá tomar as medidas necessárias para anular a ação por ele instigada.

Fica, no entanto, um ponto crucial por definir, o limite de uma possível provocação, já que há vozes às quais nos juntamos que aceitam, se bem que com muitas restrições, e outras como é o caso do acórdão supramencionado, podemos ser levados a considerar que é possível ao tribunal aceitar uma ligeira provocação, se atendermos a expressão "*sugere eficazmente ao autor a vontade de praticar o crime"* ou seja encontramos eco nas palavras de Rui Pereira, ao aceitar, em determinados casos, a provocação. Estamos aqui num patamar em que a atitude provocatória nos leva a questionar duas situações, se ela deixa um espaço de manobra podendo no provocado de decidir entre "se devo fazer", ou "não devo fazer"; ou seja, não fica apenas uma única saída, que é optar por cometer o ilícito provocado pelo agente.

1.6 AGENTE ENCOBERTO

Sobre esta figura do agente encoberto, temos na doutrina duas correntes: uma que aceita a sua existência *tout court* e outra que reconduz as figuras do agente infiltrado e encoberto a uma só figura.

Segundo Alves Meireis, a particularidade que distingue o agente encoberto das outras figuras "é a sua absoluta passividade relativamente à decisão criminosa. Estava naquele lugar aquela hora como poderia estar outro agente qualquer ou outro cidadão qualquer". Nesse sentido, "o agente encoberto é o agente de polícia ou um terceiro concertado com aquele que, sem revelar a sua identidade ou qualidade"[27], frequenta locais conotados com a criminalidade que geram intranquilidade e alarme social, como podem ser os casos de: cafés, bares, bombas de gasolina, farmácias, ourivesarias, estações de autocarros comboios, transportes públicos (elétricos, metro ou autocarros) e os demais

[27] MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal,* Coimbra, Almedina, 1999, p.192

locais abertos ao público onde exista a suscetibilidade de serem perpetrados crimes como furtos (por carteiristas, no interior de automóveis), tráfico de estupefacientes, roubos, entre outros tipos de atos criminosos.

Importa salientar que para Alves Meireis este agente encoberto não provoca o crime nem conquista a confiança de ninguém. A sua presença em nada afeta os acontecimentos, uma vez que ele apenas se desloca aos locais com a finalidade e "esperança" de poder intercetar os infratores da lei.

Valente aproxima-se das conceções de Meireis ao distinguir igualmente as duas figuras e ao afirmar que o agente encoberto "não necessita de autorização para atuar nos meandros do crime e não está restringido a qualquer catálogo de crimes."[28]

Já Isabel Oneto considera que ao "proceder-se a uma distinção entre agente infiltrado e agente encoberto, esta tinha de estar situada ao nível do tipo de operações pois haveria de operar-se no âmbito do conceito do agente infiltrado, atribuindo ao agente encoberto as operações *lightcover*. Contudo, a autora não distingue o agente encoberto do agente infiltrado, 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."[29] Completa ainda ao afirmar que "a operar uma distinção entre as duas figuras, o agente encoberto possa ser uma sub-espécie do agente do agente infiltrado.

Isabel Oneto revê na definição apresentada por Alves Meires o termo vulgarmente utilizado de "polícia a Paisana". Relembramos que a autora não faz distinção entre agente infiltrado e encoberto, pois nas suas palavras,

---

[28] VALENTE, Manuel Monteiro Guedes, *A investigação do crime organizado in Criminalidade Organizada e Criminalidade de Massa,* Coimbra, Almedina, 2009, p169

[29] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005 p140

reconduzem-se à mesma figura Só assim se entende que afirme que quando o agente (polícia e não particular) adote um comportamento passivo passa a ser um “Polícia a Paisana”. No caso do agente “à paisana”, se o mesmo, por exemplo, for abordado por um traficante de droga ou presenciar um crime, terá a obrigatoriedade de deter o ofensor em flagrante delito, situação que não se verifica no caso do agente encoberto.[30]

A figura do agente encoberto é mais tolerada formalmente, dado que recolha de prova não desrespeita a liberdade, a determinação e a capacidade de decisão do suspeito. O agente encoberto não tem qualquer ato que contribua de forma alguma para propiciar um crime, não ganha a confiança de ninguém e não tem qualquer responsabilidade na ação, a sua atitude é simplesmente passiva, ficando à espera que a ação se desenrole.[31]

A nossa posição também acompanha a visão de Isabel Oneto, no sentido em que concordamos que se a ação do agente implicar que ele próprio faça a detenção estamos perante um “Polícia a Paisana”, porque temos para nós que o agente infiltrado, quer pela sua própria segurança, quer pelo fim de recolha de informações para efeitos de prova, não efetuará detenções no decorrer da sua infiltração.

Como vimos, as expressões infiltrado e encoberto levam-nos a considerar estarmos perante duas figuras distintas, cada uma com as suas características próprias. Esta confusão pode ter origem logo na Lei 101/2001, a qual se denomina de “regime jurídico de ações encobertas”, e não de “regime jurídico de ações infiltradas”. Por outro lado, consideramos que a diferenças, caso existam, estejam ligados à forma e intensidade com que o agente se relaciona e interage com a organização sob investigação: se este se ficar pelo contacto onde se move

[30] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p139

[31] VALENTE, Manuel Monteiro Guedes, *A investigação do crime organizado in Criminalidade Organizada e Criminalidade de Massa,* Coimbra, Almedina, 2009, p169

a dita organização, estamos perante um agente encoberto; se este estiver enraizado na estrutura criminosa da organização, aí estamos perante um agente infiltrado. Uma nota adicional que fortalece a nossa posição é a de que o agente "polícia a paisana" estando num determinado espaço e tempo em que ocorre um determinado crime (como, por exemplo, injúrias a uma personalidade pública) o agente, para não relevar a sua qualidade, dá inicio a um processo para proceder à detenção do indivíduo em causa. Tal situação não é enquadrável no âmbito da lei 101/2001, por falta de respeito do princípio da proporcionalidade e mais importante é, que este crime não faz parte dos elencados no diploma.

1.7 AGENTE INFILTRADO

O Agente infiltrado é uma figura que se encontra positivada na maioria dos ordenamentos jurídicos, sendo que o ordenamento português não é exceção. É na lei 101/2001, de 25 de agosto, que encontramos o regime jurídico das ações encobertas. Apesar de ali não encontramos a expressão "Agente Infiltrado", o n.º 1 do artigo 6.º menciona o "Agente encoberto". Neste sentido, e como tomamos partido da opinião de Isabel Oneto, não distinguimos as duas figuras.

Vamos então ver o que os autores que temos anteriormente referenciados tem a dizer sobre a figura em questão.

Augusto Meireis define um agente infiltrado como um agente de autoridade ou um cidadão particular (trabalhando coordenadamente com a polícia) que, ocultando a sua identidade ou qualidade, tem como objetivo adquirir provas para a incriminação de determinados suspeitos ou apenas a obtenção de *notitia criminis*. Para tal, o agente infiltrado ganha a confiança pessoal dos suspeitos em questão, acompanha os factos que vão decorrendo,

mantendo-se informado dos acontecimentos e, se necessário, pratica atos de execução para obter a informação que se propôs descobrir inicialmente.[32]

Para Gonçalves, Alves e Valente afirmam que esta figura "convive e partilha da intimidade do suspeito, tem acesso a informações familiares e pessoais que nunca teria se não ganhasse a sua confiança, mas junta um ponto que permite distinguir entre o agente infiltrado e o agente provocador: ele age sem determinar o crime.[33]

Isabel Oneto vai no mesmo sentido que os nossos autores anteriores, definindo-o como "o agente policial, ou terceiro sob a orientação daquele, que, no âmbito da prevenção ou repressão criminal, e com o fim de obter provas incriminatórias sobre determinadas atividades criminosas, oculta a sua identidade e qualidade, podendo praticar factos típicos sem, contudo, os determinar".[34]

Já para Germano Marques da Silva, este autor aceita que se possa utilizar o agente infiltrado, mas apenas em situações de grande gravidade em que os valores fundamentais da sociedade possam ser afetados, e para atingir a realização da justiça que não seja possível através dos meios tradicionais, ou seja, meios não ocultos.[35]

Ao agente infiltrado é lhe incumbido, em primeira linha, a obtenção de informações sobre as ações dos suspeitos e da organização em que se infiltra,

---

[32] Meireis,1999, citado por GONÇALVES, Fernando, ALVES, Manuel João, VALENTE, Manuel Monteiro Guedes, *Lei e Crime – O Agente Infiltrado vs o Agente Provocador, Os Princípios do Processo Penal*, Coimbra, Almedina, 2001, p256

[33] *Ibidem,* p264

[34] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p150

[35] SILVA, Germano Marques da, *Meios Processuais Expeditos no Combate ao Crime Organizado (a Democracia em Perigo?)*. In Revista Lusíada n.º 3, 2005, p75

com o fim de permitir a recolha de provas. Está limitado, na sua ação, a atos preparatórios ou de execução não lhe cabendo, portanto, a iniciativa desses mesmos atos. Assim se evita que tais atos sejam levados como uma provocação e que criem, potencialmente, no suspeito um “animus criminalis” que não haveria ali à partida.

Como podemos constatar o recurso ao agente infiltrado para efeitos de recolha de provas ou informações que levem à obtenção de provas é pacífica, desde que não conflituem com direitos fundamentais, e que este meio de investigação seja uma exceção e não uma regra.

1.8 AGENTE INFILTRADO “O TERCEIRO”

Quando se estuda a figura do agente infiltrado uma preocupação que não pode ser afastada prende-se com a utilização do terceiro neste instrumento de obtenção de prova. Da leitura do n.º 2 do artigo 1.º da RJAE somos levados a pensar que todos os funcionários de investigação criminal e todos os particulares podem ser agentes infiltrados desde que atuem com ocultação da sua qualidade e identidade. Contudo, o n.º 1 do artigo 5.º indica-nos que só os agentes da polícia criminal é que podem atuar sob identidade fictícia. Assim sendo, somos perentórios a defender que os particulares não podem ser agentes infiltrados. Se seguirmos o pensamento de Manuel Costa Andrade e os particulares agirem apenas com ocultação da sua qualidade, então podemos enquadrá-los na categoria de homens de confiança (as testemunhas ou os informantes), mas não como agente infiltrados, uma vez que não estão todos os requisitos preenchidos para tal suceder.

O entendimento de terceiro para efeitos do n.º 2 do artigo 1.º do RJAE não parece ser o mais esclarecedor. E começa logo por não ser claro sobre quem pode ser o agente infiltrado que resulta da expressão “Funcionário de investigação criminal”. Neste ponto, não sabemos se estamos a falar apenas de OPC da polícia judiciária ou se estão aqui também incluídos os OPC da PSP e GNR. Assim, se partirmos do princípio de que o agente é reserva dos OPC, o

terceiro fica limitado aos restantes elementos policiais que não integram a investigação criminal, não alargando, por consequência, o conceito de terceiro a particulares. Não conseguimos tirar uma conclusão concreta, até porque o artigo cria uma dúvida adicional ao referir-se a “terceiro sob controlo da polícia judiciária”. Acreditamos que, por esta última citação, um não polícia, ou seja, um mero particular, possa estar abrangido.

Porém, não podemos afastar que o recurso de uma ação encoberta colide com direitos fundamentais principalmente no campo dos direitos, liberdades e garantias. Se já não é fácil aceitar que o agente seja um órgão de polícia criminal, mais difícil será se for um particular, que até pode ter um interesse pessoal na investigação do crime em questão.

Vimos este ponto com grande preocupação, por não encontramos no diploma do RJAE um cabal esclarecimento sobre quem é realmente o terceiro no enquadramento das ações encobertas. Consideramos que, a serem utilizados terceiros como particulares, que seja num noutro âmbito processual que tem estado em debate a propósito da delação premiada. Neste caso, estamos perante um informador que cede informações em proveito próprio. No entanto, impõe-se que existam regras ao seu recurso bem definidas, quais as vantagens penais oferecidas e um apertado controlo da conduta do particular. Assim perante esta situação mencionada, somos então levados a dizer que o terceiro como um particular tem cabimento.

Sabemos que a atividade de infiltração se desenvolve num leque determinado de criminalidade e que os agentes têm de ter uma preparação psicológica para o poderem enfrentar, pois as tentações de passar para o lado da delinquência estão a um pequeno passo. Como agente, terá, em última instância, a consciência do seu profissionalismo de quem é, e o porquê de ali estar. Agora, um particular é muito mais vulnerável em cair na tentação do crime: tanto pode querer ajudar a organização onde foi infiltrado como pode querer angariar dividendos em proveito próprio; isto sustenta, uma vez mais, a nossa recusa em aceitar um particular como agente infiltrado.

O recurso a particulares no âmbito das ações encobertas deve cingir-se a outros homens de confiança, como nos diz Costa Andrade, aos informadores. O uso desta figura deve, porém, ser ponderado: se, por um lado, pode ser vital para o sucesso da infiltração as informações que o informador disponibilizar ao agente que se irá infiltrar, a cautela deve imperar pelo facto de não ter outro meio para aferir a sua veracidade. Quando o informador tem conhecimento que está a meio de uma operação policial, o cuidado deve ser ainda maior. Perante isto, o informador pode exercer a sua influência em proveito próprio, tentando que a polícia afaste quem o prejudica.

1.9 AGENTE INFILTRADO PRESSUPOSTOS

Os meios ocultos, na investigação criminal representam, "uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto e nem dele se apercebam".[36] Assim, o recurso a este tipo de meio tem de ser pautado pelo respeito dos direitos fundamentais consagrados na Constituição da República. Sendo o agente infiltrado o meio que mais gravosamente pode afetar os direitos, liberdades e garantias dos visados na investigação criminal – seja ela para fins de prevenção ou repressão criminal – temos de apurar se a sua legitimidade não colide com as disposições constitucionais.

O Tribunal Constitucional, no acórdão n.º 578/98, aborda a questão da legitimidade, pronunciando-se do seguinte modo:

"Do ponto de vista da legitimidade constitucional da intervenção do agente infiltrado, é, assim, relativamente indiferente que, contra determinado sujeito, esteja ou não a correr termos um inquérito. O que verdadeiramente importa, para assegurar essa legitimidade, é que o funcionário de investigação criminal não

[36] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, A reforma do código de processo penal,* observações críticas sobre uma lei que podia e devia ter sido diferente, Coimbra Editora, 2009, p105

induza ou instigue o sujeito à prática de um crime que de outro modo não praticaria ou que não estivesse já disposto a praticar, antes se limite a ganhar a sua confiança para melhor o observar, e a colher informações a respeito das actividades criminosas de que ele é suspeito. E, bem assim, que a intervenção do agente infiltrado seja autorizada previamente ou posteriormente ratificada pela competente autoridade judiciária."

O Tribunal Constitucional vem destacar dois pontos essenciais para legitimar a atuação do agente. O primeiro é "que o funcionário de investigação criminal não induza ou instigue o sujeito à prática de um crime que de outro modo não praticaria" e o segundo é que a sua ação seja "autorizada previamente ou posteriormente ratificada pela competente autoridade judiciária".[37]

De seguida vamos olhar para o artigo 3.º do RJAE para analisar os requisitos e os pressupostos começando pelo seu n.º 1 onde temos consagrado o princípio da proporcionalidade em sentido amplo. Este princípio é, então, subdividido em três: princípio da adequação, princípio da necessidade e princípio da proporcionalidade *stricto sensu.*

O princípio da adequação explica que a ação deve ser adequada aos fins de prevenção e repressão criminal identificados em concreto, nomeadamente à descoberta de material probatório. Por sua vez, o princípio da necessidade exige que o meio utilizado seja, no caso concreto, o mais eficaz e menos oneroso. O princípio de proporcionalidade *stricto sensu* coloca frente-a-frente o meio utilizado para a prevenção e repressão criminal, e a ponderação da gravidade do crime em questão.[38]

[37] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014, p499

[38] *Ibidem,* p517

Guedes Valente acrescenta ainda dois princípios derivados da utilização dos anteriormente referidos. Assim, como consequência do princípio da necessidade, temos o princípio da subsidiariedade, segundo o qual a autoridade judiciária deve ter em conta se existe outra ação para além da encoberta que possa atingir o mesmo fim, e o princípio da exigibilidade de acordo com o qual o recurso ao agente infiltrado é a única forma de chegar à descoberta da verdade.[39]

Para apurar se os pressupostos da legalidade da ação encoberta se encontram preenchidos assim como os princípios enunciados são respeitados, não basta apenas concentrarmo-nos na conduta do agente. Para tal, carece ainda que sejam realizadas outras operações para que a legalidade da ação encoberta não seja ferida de qualquer nulidade, tanto na vertente material como formal.

É sobre a polícia judiciária que recai a competência para o controlo das ações encobertas sejam elas realizadas por funcionários de investigação criminal ou por terceiro (como nos mostra o n.º 2 do artigo 1.º, para os crimes previstos no artigo 2.º do RJAE). Tais operações de investigação criminal poderão ser realizadas sob identidade fictícia, a qual é apenas atribuída a agentes de polícia criminal, nos termos do n.º 1 do artigo 5º RJAE, sob proposta do diretor nacional da polícia judiciária ao Ministro da Justiça (n.º 2 do referido artigo).

As ações encobertas estão sob a alçada da polícia judiciária, estando, porém, dependentes de autorização judicial, se a ação encoberta estiver a ser realizada no âmbito de um inquérito. Neste caso, é ao Ministério Público que cabe comunicar ao juiz de instrução tal facto e que, caso este não profira um despacho de recusa nas 72 horas seguintes tal ação será considerada válida; se

[39] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014, p518

a ação estiver a decorrer no âmbito de prevenção criminal então é ao juiz de instrução, sob proposta do Ministério Público, que cabe aprovar essa ação n.º 3 e n.º 4 do artigo 3.º RJAE. Não estando fixado um prazo total para a duração da ação encoberta, esta é prorrogável a cada 6 meses, dado que se o agente não puder continuar a utilizar uma identidade fictícia, a operação ficará também comprometida, tal como nos refere o n.º 3 do artigo 5.º.

Concluída a operação encoberta a autoridade que controla tem um prazo de 48 horas para apresentar um relato da intervenção do agente à autoridade judiciária, de acordo com o n.º 6 artigo 3.º RJAE.

Durante a sua infiltração, o agente poderá ter de realizar algum tipo de ilícitos, ficando, como qualquer cidadão, sujeito a uma sanção criminal ou civil, conforme o caso. Porém, se a sua atividade se reconduzir a atos preparatórios ou de execução, poder-lhe-á ser imputada uma isenção de responsabilidade, segundo o n.º 1 artigo 6.º RJAE. sobre os atos preparatórios, que se realizam antes dos atos de execução do crime, estes não são, ao abrigo do artigo 21.º do Código Penal e n.º 1 do artigo 6.º RJAE, puníveis para os agentes encobertos, não sendo então necessário invocar aqui uma causa de exclusão da ilicitude. Porém, se não houvesse exclusão de responsabilidade o agente ficaria como qualquer infrator sujeito aos artigos 271.º e 275.º Código Penal.

Quanto aos atos de execução, o n.º 2 do artigo 22.º do Código Penal explica-nos que estes são os atos que, pela sua natureza, podem levar a cometer um crime. Neste ponto, o RJAE demonstra uma falta de clareza, pois não esclarece se dos atos de execução resultar um crime em concreto, o agente fica ou não sujeito a uma sanção, ou se se encontra isento de responsabilidade, ao abrigo do diploma.

Outro pressuposto é o que exclui a responsabilidade do agente, constante do n.º 1.º artigo 6.º, RJAE, de acordo com o qual os atos praticados pelo agente infiltrado sob “qualquer forma de comparticipação diversa da instigação e da

autoria mediata, sempre que guarde a devida proporcionalidade com a finalidade da mesma".

A comparticipação pode ser entendida como a colaboração ou intervenção de várias pessoas na realização de um facto. No caso do agente infiltrado, o que importa é a sua a colaboração nas atividades criminosas que se encontram sob investigação. Tendo em mente que a finalidade das ações encobertas é a recolha de prova, compreende-se aqui a lógica de aceitar que o agente esteja envolvido através da colaboração, permitindo a obtenção de prova do crime em concreto através de uma ação que não seria, de outra forma, possível.

Relativamente às formas de comparticipação segundo as quais o agente pode atuar, estas estão limitadas apenas à coautoria e à cumplicidade, porque se o fizer como autor imediato, será ele o iniciador do crime e, consequentemente, o material de prova não recairá sobre o suspeito da investigação.

A proibição de instigação e da autoria mediata é o último pressuposto que assinalamos. Sobre a instigação, vulgarmente atribuída à figura do agente provocador, sabemos que nem a jurisprudência nem a doutrina a aceitam, tirando a situação de Rui Pereira que aceita de forma ligeira e pontualmente. Sobre a autoria mediata, verificámos não lhe assiste qualquer causa de exclusão de ilicitude, uma vez que é ele o único a ter total controlo sobre o crime.

Em conclusão, o recurso ao agente infiltrado consiste num meio excecional de investigação, prevenção e repressão criminal que, apesar de poder colidir com direitos fundamentais, será admissível e legítimo desde que respeitados os termos legalmente previstos e consagrados, tanto na Constituição, como no regulamento jurídico de ações encobertas.

1.10 MODALIDADES DE AÇÕES ENCOBERTAS

Já tínhamos anteriormente feito referência às ações *light cover e deep cover* quando fizemos a distinção entre o agente infiltrado e o agente encoberto. No entanto, nessa ocasião, não foi feita uma explicação exaustiva sobre as diferentes modalidades de ações encobertas.

É na lei n.º 101/2001 de 25 de agosto que encontramos regulado o regime jurídico das "ações encobertas". Sendo esta muito abrangente, cabe aqui todo o tipo de ações através das quais se recorra a um agente infiltrado. Pode-se fazer, inicialmente, uma divisão entre dois tipos de ações, consoante a duração das mesmas: "Light cover" que, por norma, não excedem os seis meses, não carecendo, portanto, de um grande planeamento, o agente infiltrado mantêm a sua identidade, não está em contacto permanente com o meio criminoso, mantendo-se na estrutura policial (limita-se a realizar, em certos casos, uma única operação (compra, venda de estupefacientes)). As "deep cover", requerem uma preparação mais cuidada, sendo o prazo aqui superior ao das anteriores, o agente deixa a sua vida quotidiana e familiar para integrar, de forma permanente, a estrutura criminosa, sendo estas operações naturalmente mais perigosas que as anteriores.[40]

Por um lado, temos as operações light cover que podem ser divididas em seis modalidades: Decoy operation (ou operation leurre (França), a pseudo-achat, pseudo-vente, flash-roll, a livraison surveillée e a livraison contrôlée.[41]

Nas *Operation leurre,* o objetivo é, basicamente, inserir o agente no papel de vítima, num meio conhecido criminalmente, esperando que ele seja atacado por um delinquente para, posteriormente, o seu agressor ser detido em flagrante

---

[40] FERREIRA, Vanessa P. Dias, *Problèmes posés par la mise em oevre desopération sun dercover das lesdomaine de la luttecontreletrafic de stupéfiaants,* in Révue de droit Penalet de Criminologie, Ano 76, *apud,* Oneto, p81

[41] *ibidem* p82

delito pelos polícias que intervenham logo de seguida. Por seu turno, nas *pseudo-achat,* o agente é um suposto comprador de produtos ilícitos, enquanto nas *pseudo-vente*o agente é um suposto ladrão que quer vender os produtos que adquiriu de forma ilícita. Diferentemente, nas operações denominadas por *flash-roll,* o agente "exibe quantias de dinheiro aos potenciais vendedores de mercadoria proibida ou de origem ilícita, com o objetivo de 'fechar negócio'". Nas *livraison surveilée,* o agente controla uma determinada área ou atividade com o objetivo de deter os criminosos em flagrante delito. Este tipo de operações pode também ser seguido de uma *pseudo-achat* ou *flash-roll*. Nas operações de *livraison contrôlée,* são os polícias os responsáveis pela entrega dos produtos ilícitos, podendo esses produtos ser substituídos por outras coisas, ou, no caso de estupefacientes, serem trocados por substâncias inócuas[42]

Por outro lado, temos as operações deep cover que se subdividem em quatro modalidades: sting operation, honey-pot operation, buy-bust/Self-bust operation, infiltration de réseaux ou de groupes.

Primeiramente, nas *Sting operations,* o agente, sob identidade fictícia, constitui uma empresa, ou detém um estabelecimento comercial, com o intuito de vender produtos ilícitos (como armas ou joias) que podem ali ser comprados, encorajando, dessa forma, os interessados a roubar. Estas operações estão dependentes da técnica de *scouting* para poderem prosseguir, ou seja, determinados polícias fazem-se passar por ladrões e, inserindo-se em meios criminosos, publicitam o estabelecimento, com o intuito de fazer com que aqueles se dirijam ao local para comprar ou vender produtos roubados. Em segundo lugar, temos as *honey-pot operations,* bastante semelhantes às *sting opertions*, diferenciando-se apenas pelo facto de criarem um comércio (bar, café, restaurante, etc.) com o intuito de o tornar num centro para os membros de

[42] FERREIRA, Vanessa P. Dias, *Problèmes posés par la mise em oevre desopération sun dercover das lesdomaine de la luttecontreletrafic de stupéfiaants,* in Révue de droit Penalet de Criminologie, Ano 76, *apud,* Oneto ,p.83

organizações criminosas e não para comprar ou vender mercadoria ilícita. Por sua vez, as *buy-bust operations* caraterizam-se por ser uma técnica de infiltração do que propriamente uma modalidade *deep cover*, sendo esta uma operação na qual o agente obtém, progressivamente, pequenas quantidades de estupefacientes, conseguindo dessa forma obter a confiança do mesmo e inserir-se no meio criminoso. Realizada a inserção, e ganhando a confiança dos suspeitos, o agente compra uma avultada quantia de estupefacientes, a fim de, em coordenação com a polícia, deter os suspeitos da transação. Contrariamente, as *self-bust operations* caracterizam-se por ser o agente o vendedor. Por fim, a *Infiltration de réseaux ou de groupes* carateriza-se por ser uma modalidade em que o agente se insere no meio criminoso por um considerável período de tempo, com o objetivo de obter informação e provas relativas a um crime a praticar ou já praticado.[43]

1.11 CONTROLO DO AGENTE INFILTRADO

Um meio oculto de investigação criminal, que pode lesar gravemente direitos, liberdades garantias dos cidadãos, consagrados na Constituição da República, como é o caso da investigação através de agente infiltrado, não podia ficar isento de controlo judicial.

Qualquer investigação que opte por recorrer às ações encobertas, seja para fins de prevenção ou de repressão, está dependente de uma autorização prévia da autoridade judiciária competente (do Ministério Público ou do juiz de instrução criminal, nos termos do n.º 3, n.º 4 e n.º 5 do artigo 3.º RJAE). Se a ação se encontrar em fase de inquérito, cabe ao Ministério Público comunicar tal autorização ao juiz de instrução para que, nas setenta e duas horas seguintes, seja validado expressa ou tacitamente. Na base deste procedimento, dispõe o n.º 4 do artigo 32.º da Constituição da República que quando estejam em causa

[43] FERREIRA, Vanessa P. Dias, *Problèmes posés par la mise em oevre desopération sun dercover das lesdomaine de la luttecontreletrafic de stupéfiaants,* in Révue de droit Penalet de Criminologie, Ano 76, *apud,* Oneto, p84

direitos fundamentais, apenas o juiz de instrução é que tem competência; ora, se for uma situação em que a inércia do decisor origine um despacho tácito, pode-se questionar se ele chegou realmente a ter conhecimento do pedido. Porém, estando em causa restrições ao direito à reserva da intimidade da vida privada e familiar, temos que o juiz de instrução deve assumir um papel mais ativo na autorização.

Guedes Valente afirma que a inércia do juiz se reconduz a uma inconstitucionalidade material, por violação da norma do artigo 32.º da Constituição[44]. Também para Rui Pereira a intervenção do juiz em sede de inquérito é indispensável e, quando estejam direitos fundamentais em causa, aquela não pode ser delegada.[45] E tomando as palavras de Mata-Mouros, quando estamos perante meios excecionais, há que tomar cautelas adicionais.[46]

Se estivermos perante uma ação encoberta, mas agora no âmbito da investigação criminal, apesar desta se realizar mediante proposta do Ministério público, é ao juiz de instrução criminal que cabe autorizar, conforme nos indica o artigo 32.º da Constituição, conjugados com os artigos 268.º e 269.º CPP.

1.12 DEPOIMENTO E RELATÓRIO DO AGENTE INFILTRADO

Terminadas as investigações, a polícia judiciária fará, nas 48 horas seguintes, um relatório para a autoridade judicial, que só será tido como válido se o agente infiltrado tiver atuado em conformidade com os preceitos legais a que está adstrito no cumprimento da sua missão.

---

[44] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014, p522

[45] PEREIRA, Rui, "O "agente encoberto" na ordem jurídica portuguesa", *in Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa,* Vol. II, Coimbra Editora, 2005, p22

[46] MATA MOUROS, Fátima, O agente infiltrado*, in revista do ministério publico, janeiro de 2001* p108

Perante o n.º 3 e n.º 4 do artigo 5º, o agente pode prestar depoimento sob a mesma identidade fictícia com que realizou a investigação encoberta, caso seja chamado a fazê-lo a requerimento da polícia judiciária e autorizado pela entidade competente; é ao abrigo do RJAE que o agente, caso o faça, estará em tribunal como testemunha e ficará sob alçada da proteção que a Lei 93/99 atribui aos casos de testemunha protegida. Logo no seu artigo 4.º, caso as circunstâncias assim o exigem, pode a testemunha prestar depoimento com ocultação da sua identidade (voz e imagem). Ora no caso de agente infiltrado acreditamos que o seu depoimento deve ser sempre feito, sob identidade fictícia, para a sua proteção e dos seus familiares. A este respeito, ao prestar depoimento utilizando uma identidade fictícia, não parece que princípios como o do contraditório (n.º 2 do artigo 301.º do CPP) ou mesmo o princípio da mediação (n.º 1 do artigo 355.º do CPP) não sejam respeitados. De salientar que quando as testemunhas prestam depoimentos nos quais não revelam a sua identidade, o legislador é claro no n.º 2 do artigo 19 da lei 93/99 “Nenhuma decisão condenatória poderá fundar-se, exclusivamente”, como tal não consideramos que a revelação da verdadeira identidade do agente infiltrado deva ou tenha de assumir carácter obrigatório.

Sobre o relato que é elaborado num prazo até quarenta e oito horas finda a ação encoberta, este é da competência da polícia judiciária, ou seja, do órgão que controla essa mesma ação.

A investigação encoberta pode realizar-se até à prescrição do crime. Neste sentido, fazer um relato só no seu término pode ser difícil e não desejável perante a possibilidade de esta ser a única prova no seio do processo.[47]

[47] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p197

Se preocupações houve sobre questões processuais que envolvem as investigações com recurso a meios ocultos, não deixa de ser verdade que também houve alguma cautela para com os agentes infiltrados.

Guedes Valente vê a segurança dos agentes infiltrados como um domínio sensível. Quer seja pela atuação junto dos criminosos, quer por possíveis represálias, eles são merecedores de proteção, não apenas material, mas também formal, como aquela que estipula que ninguém pode ser infiltrado (apenas se o fizer de forma voluntaria e utilizar uma identidade fictícia). [48]

É inevitável dizer que o agente infiltrado se vai mover em meios criminosos e, como tal, os riscos são enormes. Seja pela sua integridade física, seja pela psicológica (e ainda pelo facto de estar sujeito a pressões de poder ser corrompido pelo meio onde se insere), toda a proteção que lhe possa ser dada, a fim de cumprir a missão e levar a que os fins da investigação tenham sucesso deverá ser considerada.

Assim, não estranhamos que ao agente infiltrado seja concedida proteção similar àquela dada às testemunhas que fazem o seu depoimento com ocultação de identidade ou ainda que durante a sua atividade de ação encoberta possam praticar qualquer ato aos quais lhe seja atribuída uma das causas de exclusão da ilicitude.

1.13 O AGENTE INFILTRADO NOUTROS ORDENAMENTOS JURÍDICOS

O Estudo sobre o nosso agente infiltrado não ficaria completo se não fizéssemos uma abordagem a outros ordenamentos. Verificar como é que os outros países lidam com esta figura permite deslindar se estamos em consonância ou se existe alguma discrepância. Caso se conclua por diferenças

[48] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014, p525

significativas entre o nosso ordenamento e os restantes, torna-se, porventura, necessário, fazer uma reflexão sobre o regime jurídico das ações encobertas e se o mesmo deveria ser questionado em algum ponto.

ESPANHA

No país vizinho, a figura do agente infiltrado está consagrada na Ley Orgânica nº5/1999, de 13 de janeiro, a qual prevê a figura do "agente encubierto" no âmbito da investigação da delinquência organizada, e amplia os meios de investigação utilizados na luta contra o tráfico de drogas e branqueamento de capitais dela derivados. No nosso ordenamento, é a Lei 101/2001 RAJE que, no seu Artigo 2º, estabelece um catálogo de crimes sujeitos a investigação comparativamente mais alargado.

O artigo 263 bis diz-nos que é da competência do juiz de instrução criminal e do Ministério Público autorizarem funcionários policiais a atuarem sob identidade fictícia numa investigação criminal, e que esta pode, nos casos urgentes, ser requerida já depois de se iniciar a investigação. Esta identidade fictícia pode, de forma idêntica à do nosso ordenamento, e ser conservada mesmo durante o julgamento.[49]

É da competência da brigada de estupefacientes a coordenação das ações preventiva e repressiva do tráfico de estupefacientes, incluindo a de todos os Corpos de segurança do Estado e dos órgãos públicos ou privados que se ocupem desta atividade. A jurisprudência espanhola admite a infiltração como meio de investigação criminal e faz, de igual modo, a separação entre o agente infiltrado e o agente provocador. Sobre a atuação do agente infiltrado, a doutrina entende que estes o fazem dentro dos limites constitucionais, sendo assim as suas condutas justificadas pelo respeito ao cumprimento dos seus deveres,

[49] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p99

admitindo assim a prática de crimes, desde que respeitado o princípio da proporcionalidade.[50]

Podemos aqui notar algumas diferenças de grande importância face ao nosso regime. Desde logo, começando pelo controlo da investigação, este não é da competência exclusiva de uma identidade judiciária. Também o princípio da proporcionalidade está presente, mas, diferentemente de Portugal, aceita-se a instigação e até o crime, dentro, porém, dos limites impostos pelo referido princípio.

Em Portugal, como já apurámos, para além dos funcionários de polícia criminal, também pode ser um particular a vestir a pele de infiltrado. Porém, no ordenamento espanhol, tal possibilidade está totalmente impedida. Entendemos que o legislador espanhol optou por não aceitar que um particular possa ser um agente infiltrado, por razões já anteriormente apontadas. Temos, por exemplo, a situação do particular na pele de criminoso: por um lado, pode ter uma melhor interação com os elementos com quem se pretende que ocorra a infiltração; mas, por outro lado, também é sabida a facilidade com que este particular se pode deixar corromper, aspeto que parece não ter sido levado em consideração pelo nosso legislador.

Sobre o relato da intervenção por parte do agente infiltrado temos aqui também uma situação ligeiramente diferente entre ordenamentos. Enquanto que, por cá, o relato só se junta ao processo caso o juiz assim o entenda, ficando assim entregue à discricionariedade da autoridade judiciária, já em Espanha o relato é junto ao processo na sua totalidade.

[50] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p.99

ALEMANHA

As ações encobertas foram introduzidas no ordenamento germânico após a aprovação da "Lei contra o tráfico ilícito de estupefacientes e outras manifestações de criminalidade organizada", de 22 de setembro de 1992. O recurso ao agente infiltrado também está aqui submetido ao princípio de subsidiariedade, embora se exija indícios que demonstrem a gravidade do crime e que o mesmo seja cometido por grupos organizados, ou que diga respeito a tráfico de armas ou estupefacientes, falsificação de moeda, documentos ou valores ou que seja respeitante à segurança do Estado. No§110b, está previsto que se a investigação tiver como objeto um certo suspeito identificado ou se exigir a entrada num domicílio particular, a autorização para a mesma é dada pelo juiz e só em casos de urgência pelo Ministério Público que pode iniciar a investigação sem a referida autorização. Porém, esta carece de posterior aprovação num prazo até três dias sob pena de ser anulada.[51]

Sobre o recurso a particulares o ordenamento alemão prevê a figura do informador e das pessoas de confiança, mas o seu âmbito não está definido na lei. Uma pessoa de confiança é alguém cuja identidade é mantida em segredo e, que sem ligação a uma autoridade policial, está disposta a auxiliar na investigação de crimes por um período prolongado. No entanto, a lei considera-os apenas como testemunhas não tendo, por isso, direitos ou deveres acrescidos em relação a outros. De uma forma geral, a jurisprudência alemã reconhece o recurso a agentes infiltrados para efeitos de investigação como admissível e também opera uma distinção entre o agente encoberto e o agente provocador, não aceitando este último. Um último ponto de referência, segundo a lei alemã o agente infiltrado não pode cometer crimes, ainda que, alguns setores, reclamem

[51] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p.97

que possa cometer pequenos delitos (caso o faça, terá de evocar uma causa de justificação ou exclusão de ilicitude).[52]

Fica deste ordenamento muito similar ao nosso, que não é permitida a instigação apesar de existirem setores que pretendem uma aproximação à lei espanhola no que concerne à possibilidade de o agente infiltrado praticar pequenos delitos.

REINO UNIDO

Neste ordenamento a atividade do agente infiltrado está vertida num código de conduta disponível para consulta pública em todas as esquadras. Segundo o referido código, as operações encobertas só podem realizar-se se estiver em causa a segurança nacional, prevenção ou deteção de crimes, manutenção da ordem pública ou da segurança da comunidade, no caso de interesse público elevado ou em cooperação com outras entidades estrangeiras. O fim primordial do recurso ao agente infiltrado é, portanto, a obtenção de meios de prova, mas também esta pode ser realizada para prevenção e deteção de crimes. O princípio da proporcionalidade também está presente, relativamente ao crime, mas também face à perigosidade do suspeito. Algo inédito em relação aos restantes ordenamentos, é o alerta relativo aos riscos de intromissão na privacidade dos cidadãos que não são alvo direto da investigação (intromissão colateral). As operações encobertas constam de documento escrito, tendo uma validade máxima de três meses, (com possibilidade de renovação), sendo que, em situações de urgência, pode haver autorização oral válida até 72 horas. No ponto 1.10 surge a proibição de provocação ao crime assim como a instigação a crimes para os quais não exista uma predisposição por parte do agente.[53]

---

[52] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p98

[53] *Idibem* p105

Visto este regime jurídico e tirando a questão dos danos colaterais, ele parece-nos em tudo semelhante ao português.

ESTADOS UNIDOS

Neste país, as ações encobertas revestem grande importância, mas, perante uma criminalidade evoluída, a implementação de agentes infiltrados no terreno não é fácil, pois muitas organizações criminosas adotam como rituais de iniciação, tais como a prática de homicídio. [54]

Assim, não estranhamos que o sistema jurídico americano atribua imunidade geral aos agentes no exercício das suas competências em operações encobertas. É no código federal, capítulos 13 (prevenção e controlo) e 21 (alimentos e drogas) que encontramos a regulamentação sobre as ações encobertas para o caso de tráfico de droga, embora estas possam ser extensíveis a outros tipos de crimes. O pagamento a informadores está legalmente previsto, bem como a compra de estupefacientes. É igualmente permitida a criação de empresas falsas no âmbito de uma investigação criminal, como foi o caso "ABSCAM", no qual falsos investidores imobiliários procuravam apurar atos de corrupção na classe política.[55]

BRASIL

No Brasil, foi em 1995 que surgiu a primeira tentativa de consagrar a figura do agente infiltrado através da lei n.º 9.034 para a prevenção e repressão da criminalidade organizada. Com a Lei 10.217, e juntamente com outros meios de investigação como a captação e interceção ambiental de sinais eletromagnéticos, óticos ou acústicos, bem como o seu registo e análise (ainda que sujeito a

---

[54] GROPP,W.,*Special Methods of Investigation for Combating Organized Crime, in European Journal of Crime, Criminal Law and Criminal Justice* ,Lisse (Holanda), 1993, p33 *apud* ONETO, Isabel, *op.cit*., p.96

[55]*Ibidem*, p106

autorização judicial), é introduzida a figura do agente infiltrado. Se o sistema português consagrou um diploma apenas com sete artigos para ações encobertas, o sistema brasileiro foi ainda mais simplista, já que faz apenas uma referência à figura do agente infiltrado na lei das drogas. Este ordenamento exclui os particulares da investigação, sendo necessária uma autorização judicial e sigilosa que permita que o crime, desde que cometido por uma organização criminosa, possa ser investigado com recurso ao agente infiltrado, não existindo um catálogo de crimes taxativo como em Portugal.[56]

Tínhamos dito que a figura do agente infiltrado está praticamente positivada na maioria dos ordenamentos jurídicos. Ora, a Colômbia constitui uma exceção a esta tendência uma vez que não admite a figura do agente infiltrado, permitindo apenas que seja premiada a cooperação e a delação com a redução de um a dois terços da pena, e ainda recompensas em dinheiro.[57]

[56] ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005, p107

[57] *Ibidem*, p108

2 CAPÍTULO II - O AGENTE INFILTRADO EM MEIO DIGITAL

2.1 SOCIEDADE DA INFORMAÇÃO

O Homem é, por natureza, um ser incansável na procura de melhores condições de vida para o seu dia a dia, melhorando o seu conforto. De modo a alcançar este propósito, ele pode concentrar o seu foco em dois pontos: por um lado, realizar as suas tarefas com recurso ao mínimo de meios necessários e, por outro, pode fazer com que essas sejam executadas com a maior brevidade possível. Este objetivo da sociedade é exequível, de ser realizado, seja através do que a natureza lhe oferece ou, meramente, através do que seu génio consegue inventar.

Ao longo da história temos marcos que alteraram profundamente a vida da sociedade, como é disso caso a revolução industrial através da “Máquina” a qual marca uma mudança na sociedade. O Homem passou a consumir bens e a dispor de tempo que até aí não dispunha como resultado direto do aumento da oferta a custos mais reduzidos. A máquina é um dos vários meios a auxiliar o Homem nas suas tarefas e, na era do mundo das tecnologias da informação, temos ferramentas como o computador, o tablet ou o smartphone, que continuam a permitir que o homem satisfaça as suas necessidades com pouco esforço físico e grande rapidez.

A peça fulcral nesta era da informação é, sem dúvida, o computador. Não é pacífica a paternidade do computador moderno, sendo ela atribuída ora a Howard H. Aiken em 1937, ora a Atassnoff e Berry em 1940. Independentemente do facto a quem pode ser atribuída a sua origem, é com a 2ª guerra mundial que o computador vai registar um grande salto tecnológico, operado em cinco gerações.[58]

[58] ROSSINI, Augusto, *Informática Telemática e Direito Penal,* Memória Jurídica Editora, São Paulo, 2004, p24

Na primeira geração, entre 1940 a 1952, temos os enormes computadores de uso exclusivamente militar. Fruto da sua conceção, à base de válvulas a vácuo e alimentação da informação por cartões perfurados, estes permitiam fazer de forma rápida cálculos complexos através da programação dos seus circuitos elétricos.[59]

A segunda geração, de 1952 a 1964, inicia-se com a substituição das válvulas por transístores, reduzindo assim significativamente o seu tamanho e operando um aumento da rapidez de execução dos cálculos que lhe eram submetidos.

Na terceira geração, entre 1964 e 1971, surgem os circuitos integrados que vêm substituir os transístores, reduzindo-se ainda mais o tamanho das máquinas. Verifica-se também uma evolução do software e dá-se a criação de chips de memória. Com estas transformações, o seu uso começa a deixar de ser apenas militar e académico, passando também agora a ter uma finalidade comercial.

A quarta geração, de 1971 a 1981, na sequência da redução do tamanho da máquina é, precisamente, a substituição dos circuitos por microprocessadores, surgindo também os dispositivos de armazenamento, vulgarmente conhecidos como disquetes. Até aqui, cada máquina tinha o seu próprio software, e é a IBM que põe fim a esta prática.[60]

De 1981 em diante, entramos na última geração, tendo como foco a inteligência artificial e a disseminação da internet.[61]

---

[59] Saaveda, Rui, *A Proteção Jurídica do Software e a Internet,* Sociedade Portuguesa de Autores, Publicaçoes Dom Quixote, Lisboa, 1998, p42

[60] *Ibidem*, p42

[61] ROSSINI, Augusto, *Informática Telemática e Direito Penal,* Memória Jurídica Editora, São Paulo, 2004, p25

Com a criação do computador, vai se dar uma nova revolução, a terceira denominada era da informática. Os anos oitenta trouxeram mudanças radicais na vida da sociedade, como é disso exemplo as inovações no setor da banca, onde as pessoas deixam de ter necessidade de se dirigirem aos balcões para levantar dinheiro e passam a realizar os seus levantamentos nos multibancos disponíveis 24 horas. Ao nível do setor administrativo, o computador tem um impacto profundo em certos casos como na correção dos documentos datilografados e na substancial redução no gasto de papel. Outro exemplo, dos muitos que podemos dar sobre a radical influência do computador na vida do Homem, é no setor do comércio, por intermédio do registo das compras feito através de um leitor ótico de código de barras, que permite que seja mais rapidamente atendido.

Se esta revolução já teve um grande impacto na sociedade, a quarta revolução – da era digital ou da sociedade de informação – tem o seu início com a interligação dos computadores, fomentando o aparecimento de uma nova ferramenta, a *"Internet"* e a criação do ambiente digital ou do ciberespaço.[62]

A internet reporta a sua génese, assim como no caso do computador, ao campo militar. Com a finalidade de proteger a rede de computadores do governo norte-americano no período da guerra fria, surge, em 1967 a ARPANET, precisamente para proteção da sua rede em caso de ataque nuclear.

No campo académico, as universidades da Califórnia, Los Angeles e Santa Bárbara, em conjunto com a universidade de Utah e o SRI de Stanford, em 1969 via "*Backbones",* consegue que estes quatro "*hosts"* se interliguem. A estes, juntam-se, mais tarde, em 1971, agências governamentais e militares americanas, incluindo a NASA. É no ano imediatamente seguinte que é lançado o primeiro programa de correio eletrónico, hoje em dia vulgarmente conhecido

[62] A palavra "ciberespaço" surge da aglutinação dos termos "cibernética" e "espaço". Avançada inicialmente pelo escritor canadiano William Gibson, no seu livro "Neuromencer" (1984)

por e-mail, antecedendo a primeira ligação transcontinental entre Inglaterra e os Estados Unidos.

No âmbito comercial, é criada em 1979 a Usenet, uma rede descentralizada de grupos de notícias, na qual são incorporadas conexões de radio e satélite. Em França, aparece a rede Minitel – que por motivos técnicos acabou por nunca sair de dentro das suas fronteiras – já permitia a transmissão de mensagens e jogos através da rede da France Telecom.

O grande evento que veio dar novo impulso à internet, em 1982, através do estabelecimento do protocolo IP/TCP, foi a interligação de todas as redes existentes assim como dos seus respetivos computadores. Paulatinamente, diversos países foram se interligando numa mesma estrutura, a NSFNET – a atual base da internet – que rapidamente cresceu até ao nível que hoje conhecemos, com a interação constante dos países que não o fizeram inicialmente.

O surgimento de meios tecnológicos tem permitido uma constante evolução na qualidade do dia-a-dia da sociedade. Se até à revolução industrial o impacto nas comunidades levou um tempo considerável, com o surgir dos meios das tecnologias da informação, essa evolução foi exponencial. E nem os mais otimistas poderiam prever o quanto estas tecnologias se tornariam indispensáveis.

A revolução da era digital surgiu para facilitar a vida em sociedade, mas depressa conquistou os setores ligados a atividades menos lícitas, facilitado pela internet que consegue interligar os dispositivos de forma instantânea, permitindo comunicar a uma velocidade estonteante para todo o mundo e de forma anónima.

2.2 CIBERESPAÇO E OS SEUS DESAFIOS

Não podíamos deixar de fazer referência no nosso trabalho à noção de ambiente digital, também designado por ciberespaço, assim como das suas características, pelo motivo de ser este o meio em que a nossa figura do agente infiltrado se movimenta.

Já tínhamos anteriormente afirmado que o termo ciberespaço surge referenciado na obra de ficção científica de William Gibson “Neuromancer”, sendo este definido como uma rede de computadores que dá origem a um ambiente no qual circula uma enorme quantidade de informação e onde os utilizadores poderiam vivenciar ambientes ficcionados com efeitos no mundo real.

A visão de Gibson é a de que a maioria dos utilizadores mais se identifica sobre o que é o ciberespaço, em que temos pontos de acesso (computadores smartphone, etc.) a uma quantidade de informação, mas este ambiente vai mais longe, ao ponto que não gere um consenso alargado como podemos verificar pelas diversas noções que apresentamos em seguida.

O Departamento de Defesa Norte Americano designa o ciberespaço 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.[63]

Michael Benedick propõe na sua obra “Cyberspace: First steps” uma definição de ciberespaço: *“Ciberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multidimensional, artificial, or "virtual" reality. In this reality, to which every computer is a window,*

[63] Department of Defense Dictionary of Military and Associated Terms p58, consultado em https://fas.org/irp/doddir/dod/jp1_02.pdf

seen or heard objects are neither physical nor, necessarily, representations of physical objects but are, rather, in form, character and action, made up of data, of pure information. This information derives in part from the operations of the natural, physicalworld, but for the most part it derives from the immense traffic of information thatconstitute human enterprise in science, art, business, and culture.The dimensions, axes, and coordinates of cyberspace are thus not necessarily the familiarones of our natural, gravitational environment: though mirroring our expectations ofnatural spaces and places, they have dimensions impressed with informational valueappropriate for optimal orientation and navigation in the data accessed."[64]

Para este autor, o ciberespaço é um novo e paralelo universo, criado e mantido por computadores e linhas de comunicação, onde circulam conhecimentos e segredos. É uma realidade virtual, presente, ao mesmo tempo, em qualquer lugar e em lugar algum.

Não existe consenso sobre uma definição uniforme e universal de ciberespaço, mas podemos identificar algumas características. Assim, existe um consenso generalizado de que ele não se confunde com a internet, apesar de ser o seu principal e mais relevante ambiente. Neste sentido, o ciberespaço consiste, não só na Internet e nos computadores a ela ligados, mas também nos sistemas e equipamentos eletrónicos ligados com outros equipamentos ou

[64] Consultado em http://mbenedikt.com/royal_swedish_academy.pdf p4, "*O Ciberespaço é uma realidade globalmente conectada em rede, sustentada por computador, com acesso por computador e gerada por computador, multidimensional, artificial ou "virtual". Nessa realidade, para a qual todo computador é uma janela, os objetos vistos ou ouvidos não são nem físicos nem necessariamente representações de objetos físicos, mas sim, em forma, caráter e ação, compostos de dados, de informação pura. Essa informação deriva em parte das operações do mundo natural, físico, mas em grande parte deriva do imenso tráfego de informações que constituem o empreendimento humano em ciência, arte, negócios e cultura. As dimensões, eixos e coordenadas do ciberespaço são: portanto, não necessariamente as palavras familiares de nosso ambiente gravitacional natural: embora espelhando nossas expectativas de espaços e lugares naturais, elas têm dimensões impressas com valores informacionais apropriados para orientação e navegação ideais nos dados acedidos."*

sistemas com quem partilham a mesma estrutura de energia. Temos ainda a perceção da perda de uma presença física, pois tudo desenrola maioritariamente no domínio ou ambiente virtual, num anonimato quase total. A noção de desmaterialização é imediatamente constatável porquanto no ciberespaço, na sua dimensão virtual, não há matéria, não existe nada de físico, tudo circula, flui e se armazena no ambiente virtual citado. Também a perspetiva de territorialidade é alterada, uma vez que não existem fronteiras para a comunicação, para a transmissão de dados.

Estas características entram em conflito com qualquer sistema normativo que tenha a sua base assente em dois princípios fundamentais: o Princípio da Territorialidade e o Princípio da Soberania.

O primeiro princípio traduz-se nas fronteiras territoriais (geográficas) que delimitam áreas, dentro das quais diversos conjuntos de normas são aplicáveis. O segundo princípio está relacionado com a necessidade de existência de uma autoridade investida de poderes para fiscalizar a aplicação de normas e, em caso de desrespeito, sancionar a infração.

A Internet trouxe consigo importantes fatores que põem em causa princípios jurídicos, tais como o aspeto transnacional de uma rede que não conhece fronteiras nacionais e a desmaterialização da informação. Perante o domínio digital e as novas realidades do ciberespaço, os Estados sentem-se ineficazes na aplicação do seu Direito interno. Acreditamos que este é um dos grandes desafios que o Direito enfrenta, mas também um enorme ponto de aproveitamento para a realização de ilicitudes.

Nestes tempos da era da informação, a Internet é um excelente veículo para as organizações com interesses na pedofilia ou no tráfico de seres humanos, na prostituição, bem como para todos os tipos de seitas religiosas. Perante o acesso rápido e desprotegido à informação, torna-se fácil para estas entidades conseguirem encontrar novos alvos, no primeiro e segundo caso, bem como novos interessados e afiliados, no terceiro caso. Se estes atores

pretenderem aumentar a possibilidade de não serem descobertos pelas autoridades, existem ainda outras redes como a “Darket”, na qual grande parte dos conteúdos se encontra indisponível para a maioria das pessoas, por ser necessário uma senha de acesso que dá entrada numa quase “secreta” Internet.

Outras vantagens emergem diariamente nesta era da globalização como não termos necessidade de procurar por certos serviços, já que estes vêm até nós. São disso exemplo as facilidades bancárias para pedir empréstimos aos bancos que são enviadas diretamente para as nossas caixas de correio ou as compras on-line que nos possibilitam uma maior qualidade de vida e comodidade se pensarmos no desperdício de tempo que as levaríamos a fazer, proporcionando-nos tempo para outras atividades. Porém, em sentido inverso a todas estas facilidades que surgiram, temos o reverso da moeda que nos mostra episódios de crianças que são levadas até aos pedófilos ou de mulheres que são levadas até aos clientes para prestarem serviços de prostituição, em muitos casos, contra a sua vontade e sob ameaça de represálias.

De igual forma, o aumento da partilha de informação pessoal na Internet quer de imagens, fotografias, vídeos, relatos de atividades do dia-a-dia, através das redes sociais, tem também gerado novos desafios para o Direito, já que são cada vez mais os casos de extravio desses dados pessoais, furto de identidade ou de casos mais graves, como o Cyberstalking.

Por fim, cabe referir aquela que consideramos ser uma crescente ameaça do Ciberespaço: o Ciberterrorismo. Esta é uma ameaça cada vez mais comum e global que usa a Internet como meio de propaganda, para transmitir as suas mensagens, para causar o terror e como forma de recrutamento de novos afiliados, infiltrados e seguidores por todo o mundo. O principal epicentro deste fenómeno e talvez o mais catastrófico de todos os tempos foi o atentado de 11 de setembro às torres gémeas nos Estados Unidos da América, que colocou o mundo em constante alerta, com transmissões em direto dos próprios atentados.

As situações de risco apresentadas são realidades que no ciberespaço ganham contornos de globalização numa escala que acarreta grandes dificuldades de resolução para o Direito.

2.3 LEI DO CIBERCRIME

Foram precisos completar oito anos sobre a Convenção de 23 de novembro de 2001 de Budapeste para que Portugal procedesse à sua ratificação, através da Resolução da Assembleia da República nº 88/2009 e pelo Decreto do Presidente da República nº 92/2009. A Convenção sobre o Cibercrime é considerada o primeiro e mais importante trabalho internacional de fundo sobre "crime no ciberespaço", um dos instrumentos legislativos que serviu de modelo para a Lei nº 109/2009, de 15 de setembro, mais conhecida por "Lei do Cibercrime", transposto para o direito interno através da decisão-quadro nº 2002/222/JAI, do conselho de 24 de fevereiro.

Uma das lacunas que a lei do cibercrime – que revogou a lei da criminalidade informática – veio colmatar foi a de um regime que regulasse de forma específica e detalhada o modo de obtenção de prova digital. Não significa isto que até à aprovação desta lei houvesse um vazio legal sobre prova digital; à época, era o código de processo penal que solucionava o caso, reconduzindo todas as comunicações transmitidas por meio diferente de telefone ao regime das escutas, o que gerava dúvidas, quer na doutrina, quer na jurisprudência.[65]

Em matéria de disposições penais materiais, o legislador excluiu o catálogo de crimes informáticos do Código Penal, mantendo o catálogo de crimes de Devassa por meio de informática e de Burla Informática, consagrados nos artigos 193.º e 194.º CP, respetivamente. No Capítulo I, define o artigo 1º que "A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal,

[65] MESQUITA, Paulo dá, *Processo Penal, Prova e Sistema Judiciário,* 1ª ed., Coimbra Editora, setembro 2010, p102

relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico. No art.º n.º 2 temos algumas definições como "sistema informático, dados informáticos, dados de tráfego, fornecedor de serviços, interceção, topografia e produto semicondutor". No capítulo II a Lei do Cibercrime engloba entre os artigos 3.º e 8.º, os crimes de Falsidade Informática, dano relativo a programa ou outros dados informáticos, Sabotagem Informática, Acesso Ilegítimo, Interceção Ilegítima, e Reprodução Ilegítima de programa protegido.

O artigo 11.º estabelece o âmbito material de aplicação das disposições processuais previstas no Capítulo III. A este propósito, Pedro Venâncio afirma que as medidas processuais de recolha da prova digital previstas na Lei do Cibercrime têm um campo "de aplicação geral", na medida em que estamos perante a possibilidade de recurso a estes "meios de obtenção de provas digitais para o combate da criminalidade, seja qual for a sua forma."[66] Estamos assim, perante um regime processual de obtenção da prova digital com um campo de aplicação mais abrangente e não apenas restringido a processos relativos a crimes informáticos, bastando que a prova esteja em formato digital ou em dispositivos informáticos.

No entanto, o artigo 11.º exceciona a aplicabilidade dos artigos 18.º e 19.º, tendo estes dois artigos um âmbito de aplicação bastante mais restrito que os demais meios de obtenção de prova previstos no Capítulo III. Tal exceção justifica-se pelo carácter bastante intrusivo destas duas diligências. O artigo 19.º é, de longe, o que mais nos importa nesta lei, já que o legislador incluiu um regime inovador, permitindo a abertura de ações encobertas à investigação forense. Pedro Venâncio defende aqui que este catálogo de medidas processuais deverá ser considerado de forma integrada, "analisado como um

[66] VENÂNCIO, Pedro Dias, "JusJornal" N.º 1182, 23 de Fevereiro de 2011, Editora Coimbra Editora, grupo WoltersKluwer

todo, pois em muitos aspetos práticos se relacionam e complementam"[67], visando o mesmo objetivo de aceder a dados informáticos necessários à investigação.

O legislador português, através deste artigo n.º 19, alargou mais ainda, as disposições sobre as ações encobertas em meio digital. Ficam assim abrangidos os crimes passíveis de investigação através de ações encobertas: os consagrados no RJAE assim como os elencados no artigo 19.º para os crimes previstos na Lei n.º 109/2009 e para crimes cometidos através de meio informático – correspondente a uma pena de prisão superior a 5 anos, ou inferior, se revelarem dolosos – tais como crimes contra a liberdade e a autodeterminação sexual de menores ou incapazes, burla qualificada, burla informática e nas comunicações, discriminação racial, religiosa ou sexual e infrações económico-financeiras.

Dá Mesquita apresenta duas críticas referentes a esta norma. Se, por um lado, o legislador ampliou de forma contundente o catálogo de crimes previsto no artigo 2.º do Regime Jurídico das Ações Encobertas, por outro, passa a prever uma medida excecional para um vasto conjunto de crimes – alguns de pequena criminalidade – sem aprofundar normativamente os princípios da proporcionalidade e da necessidade. [68]

Rita Castanheira Neves segue a mesma linha de pensamento, considerando que a "atitude legislativa de flexibilização de alguns princípios básicos na condução da investigação criminal" acabam por fazer com que "cada

[67] VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, 1.ª ed., Coimbra, Coimbra Editora, 2011, pág99.

[68] MESQUITA, Paulo dá, *Processo Penal, Prova e Sistema Judiciário,* 1ª ed., Coimbra Editora, setembro 2010, p126

vez mais se arrisque que o Estado perca a sua superioridade ética relativamente ao criminoso.[69]

O capítulo IV diz respeito à cooperação internacional. Como já referido anteriormente, a falta de fronteiras físicas no mundo digital cria obstáculos à investigação criminal e à aplicação do Direito. Por isso, os artigos 20.º a 26.º tendem a criar soluções internacionais de combate ao cibercrime. A este propósito, a convenção impôs à polícia judiciária a criação de uma estrutura que garante um ponto de contacto sem interrupção entre as autoridades nacionais com as autoridades internacionais, como nos explica o art.º 21 da Lei do cibercrime.

Prevista está também a possibilidade de poder ser solicitada a Portugal a preservação e revelação expedita de dados informáticos art.º 22.º - armazenados em sistema informático relativo a crimes previstos no art.º 11.º. Este comando normativo tem como objetivo a apresentação de um pedido de apoio judiciário para fins de pesquisa, apreensão e divulgação de dados. Em qualquer caso, tal solicitação dirigida às autoridades portuguesas pode ser recusada, caso os dados respeitem a infração de natureza política ou conexa, atentem contra a soberania, segurança ou ordem pública, ou ainda quando não sejam oferecidas garantias adequadas à proteção dos dados ou, finalmente, quando se concluir que faltará o requisito de dupla incriminação. Estes são os motivos de recusa constantes do art.º 23º da LC.

Adicionalmente, as autoridades estrangeiras podem formular um pedido às autoridades portuguesas para que seja autorizada pelo juiz a interceção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que esta medida esteja prevista em acordo,

[69] NEVES, Rita Castanheira, *As ingerências nas Comunicações Eletrónicas em Processo Penal,* 1ª ed., Coimbra editora, 2011, p282.

tratado ou convenção internacional e que seja admissível ao abrigo do art.º 18.º da LC. – Interceção de comunicações em cooperação internacional – art.º 26.º

A lei do cibercrime termina com o capitulo V que dispõe sobre a aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses art.º 27.º, sendo que a lei penal portuguesa é aplicável nos casos previstos no CP, tratados ou convenções internacionais e ainda aplicável a factos enumerados no seu n.º 1. No caso de existir um conflito positivo de competências (situação na qual dois tribunais se consideram competentes para conhecer de um dos crimes previstos na LC), deve recorrer-se aos mecanismos instaurados no seio da União Europeia previsto no n.º 2 do artigo citado, e decidir em que tribunal o processo vai ter seguimento, sendo que este toma a sua decisão de aceitação ou transmissão têm de atender aos fatores elencado no nº3. É aplicável com as necessárias adaptações as regras gerais de competência previstas no CPP, n.º 4 art.º 27 Lei cibercrime, sendo que, em caso de dúvida, a competência cabe ao tribunal que primeiro tiver conhecimento dos factos. Em tudo o que não se encontrar previsto na LC são aplicáveis as disposições do CP, CPP e da Lei nº144/99 de 31 de agosto (Lei da cooperação judiciária internacional em matéria penal), art.º 28º Regime geral aplicável. A competência da polícia judiciária em cooperação internacional, para efeitos da presente lei, é desenvolvida no âmbito da Unidade do Cibercrime – unidade orgânica que investiga os crimes previstos na LC. art.º 29.º. Para proteção de dados pessoais é aplicável ao seu tratamento o previsto na Lei nº 67/98 de 26 de outubro art.º 30º.

A entrada em vigor da LC operou a revogação da Lei nº 109/91 de 17 de agosto lei da criminalidade informática.

2.4 ORDENAMENTO ESPANHOL

O Governo espanhol para fazer face ao aumento dos delitos realizados com o auxílio da internet através do recurso das novas tecnologias da informação e da comunicação, passou a contemplar a figura do agente encoberto informático.

A lei orgânica de 5/1999, de 13 de janeiro alterou a “ley de Enjuiciamento Criminal” em matéria de aperfeiçoamento da ação de investigação relacionada com o trafico de droga e outros ilícitos graves, em que consagrou a figura do agente encoberto no articúlo 282 bis de LECrim, situando-se no livro II, Título III com epigrafe “La Policía judicial”. A lei 13/2015 de 6 de dezembro veio introduzir a figura do agente encoberto informático, assim como, a regulação do agente nas comunidades privadas em ambiente de rede e a regulação das respetivas gravações entre agente e suspeito.

Com a internet a criar dificuldades para a deteção e investigação dos delitos, em muito pelo anonimato que possibilita, associando em alguns casos, falta de medidas de segurança dos seus utilizadores e principalmente quando as condutas ilícitas entram no campo transnacional. Assim, o agente encoberto informático é visto como uma medida idónea no combate de certos crimes como a pornografia infantil, ou de interceção de comunicações no seio de organizações criminosas.[70]

É segundo Lafont Nicuesa pacifico que o campo de atuação do agente encoberto informático se centra por um lado nas comunidades abertas, “ciberpatrullaje”, e por outro nas comunidades fechadas.[71] Ele faz referência no primeiro caso quando agente encoberto atua com identidade fictícia com o objetivo de encontrar crimes sem que para isso esteja em curso uma investigação em concreto ou mesmo suspeitos identificados. No segundo caso, já será a conduta do agente regulada pela LECrim quanto ao envio de material ilícito nas comunidades fechadas, sobretudo perante crimes de pedofilia.

O Campo de atuação das “Ciberpatrulhas” é a vigilância, prevenção e evitar os ilícitos nas redes de fonte abertas, em que qualquer utilizador terá

[70] FERNANDEZ TERUELO, J., *Cibercrime. Los delitos cometidos a través de internet, Constitutio Criminalis,* Carolina, Oviedo, 2007, p13

[71] NICUESA, Luis Lafont, *El agente encuiberto en el proyecto de reforma de la ley de Enjuiciamento Criminala,* 2015, p2

acesso, tendo em conta que não houve nenhuma restrição na sua publicação na rede. Sendo o acesso livre, o agente encoberto informático não precisa de autorização judicial prévia para atuar, ou conquistar a confiança do criminoso.

Caso a atuação do agente sejam dentro de comunidades fechadas a utilização do agente é não só para os crimes contidos no artigo 282 bis. 4 LECrim mas também os previstos no 588 ter a), da mesma lei em que se destacam os *"Cometidos a través de instrumentos informáticos o de cualquier tecnologia de la informacíon o la comuniccíon o serviço de comunicacíon"* o campo de atuação é alargado não ficando circunscrito a criminalidade organizada.

A necessidade de combater a pedofilia na internet em fóruns de acesso restrito em que é mais difícil um controlo policial eficaz, veio a Fiscalía Provincial de Madrid (Ministério das finanças de cada região) no seu relatório de 2010 afirmar que para estas investigações seriam necessárias o recurso ao do agente infiltrado ou outros meios de infiltração para conseguir identificar os suspeitos e recolher prova digital para a respetiva incriminação.

Como é de conhecimento geral, a entrada em fóruns privados é feita por convites, e para que o agente consiga ter a confiança do suspeito tem de fazer prova que também ele é pedófilo entregando material pornográfico para conquistar a confiança do administrador do fórum. Ora a jurisprudência aceita este ilícito por parte do agente desde que respeito o princípio de proporcionalidade, verificando previamente que esta perante uma atividade ilícita[72], assim como a doutrina desde que seja mesmo necessário para o agente se infiltrar no seio do grupo de pedófilos.[73]

[72] STS 767/2007 3 outubro 2007

[73] DE LA ROSA CORTINA, J.M., "Los delitos de pornografía infantil. Aspectos penales, procesales y criminológicos, Tirant lo Blanch, Valencia, 2011

Perante isto, a Fiscalía Provincial de Madrid determinou que devia-se regular o tipo de arquivos ilícitos que podem ser alvo de troca com os suspeitos, assim como o seu destino e o controlo sobre eles na rede, podendo ter uma melhor perceção pelo princípio da proporcionalidade.

Um ponto em que a lei parece ter criado uma lacuna é no caso de ser o agente infiltrado a realizar as gravações de imagens e som ou se é a equipa de apoio do agente na investigação. Entre o agente e o suspeito a obtenção de gravações seja de áudio ou imagem ter que ter uma autorização previa do juiz de instrução artículo 282 bis 7 LECrime, no caso de as mesmas se realizar pela equipa que apoia o agente não há uma referência clara na lei, e como tal o artículo 588 quarter a, em que as gravações carecem de ordem judicial, não esta vocacionado para as equipadas de apoio, mas sim para qualquer gravação pretendida.[74]

2.5 ORDENAMENTO BRASILEIRO

No Brasil a lei 13.441/17 acrescentou à lei 8.069/90, estatuto da criança e do adolescente, o artigo 190-A permitindo o recurso a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de crianças e adolescentes. O artigo é taxativo sobre quais os crimes que podem ser sujeitos a figura do infiltrado na internet, e tem a particularidade que só é permitido para investigação com o suspeito concreto e não permite a prevenção.

O legislador optou por um permitir apenas para efeito de investigação que o agente infiltrado na internet possa ser utilizado deixando de fora para as situações de prevenção, ao contrário do que fez o legislador espanhol, perante a gravidade do crime em causa, acreditamos que não foi a melhor solução.

O artigo introduzido é claro sobre a necessidade de autorização prévia para o recurso do infiltrado, mas antes tem que ser respeitado o princípio da

[74] NICUESA, Luis Lafont ,op., cit., p. 6

subsidiariedade, ou seja, só em *último ratio* é que pode ser este meio autorizado, assim acontece também com a lei 11.343/06 e 12.850/13 em que os meios de investigação podem colidir com direitos fundamentais.

A duração deste tipo de operações é de 90 dias renováveis por iguais períodos até 720 dias, ou seja, aqui também são aceites as operações light cover ou deep cover, apenas tem que ser fundamentadas as renovações e o juiz proceder a sua autorização. Ora acrescentamos que tendo o juiz a faculdade de pedir relatórios parciais antes do termino da operação deveriam estes serem necessários quando se procedesse as renovações, permitindo não só verificar os argumentos de novo prazo assim como inteirar-se da legalidade dos atos dos agentes.

A finalidade da infiltração virtual e, consequentemente, do agente infiltrado, no ordenamento brasileiro não é disseminar práticas criminosas, induzir pessoas a cometer atos ilícitos, mas sim desvendar a existência dessas práticas permitindo a punição de seus autores, os quais optaram, de livre arbítrio, pela realização de ilicitudes, aqui não é permitido a provocação ou instigação, ou seja, segue em sentido contrário a lei espanhola.

Mas volta a ter um ponto comum quanto ao requisito de autorização judicial se tiver no âmbito de fontes fechadas sendo dispensável se forem fontes abertas, assim como a criação de perfil falso de usuário para recolha de dados. Isso porque, para interagir na internet, o utilizador aceita abrir mão de grande parte de sua privacidade. Logo, nada impede que o agente crie um utilizador falso para aceder a informações públicas (pois foram disponibilizadas voluntariamente) como fotos, mensagens, endereço, nomes de amigos e familiares.

Uma nota importante é sobre a validade da prova obtida por agente infiltrado virtual só é validade se tiver sido respeitado o princípio da subsidiariedade. Nos casos em que seja violado o princípio supracitado, já que

seria possível a recolha da prova por outros meios de investigação, a prova então obtida não será valida para efeito de processo.

2.6 CASO "SWEETIE" [75]

A pedofilia é um crime que prolifera pelo mundo inteiro, e o ambiente cibernético não fica alheio a este flagelo, potenciado pela facilidade do anonimato que a rede permite aos predadores. Com a pretensão de demonstrar este problema do abuso sexual de menores na internet uma OMG holandesa "Terre des Hommes" desenvolveu um programa com uma criança virtual de 10 anos, a menina "Sweetie".

Durante 10 semanas a criança virtual foi abordada por 20 mil contactos de adultos, prováveis abusadores sexuais, destes, mil foram localizados e denunciados à Interpol, constando da lista 3 pessoas que abordaram Sweetie a partir de Portugal.

O negócio de abuso sexual de menores na internet estima-se ser mais proveitoso que a pornografia infantil, e segundo o FBI e a ONU circulam 750 mil predadores abusando através de webcams de crianças a partir dos 6 anos. A dificuldade de provar este crime é bastante elevada, assim se pode aferir por terem apenas acusado 6 homens. Para aumentar a taxa de sucesso, a OMG "Terre des Hommes" surgirem que o agente infiltrado seja um meio a aplicar neste tipo de crime como forma de apanhar os predadores em flagrante delito.

O modelo de abordagem elaborada pela organização foi através da criação de um perfil de uma menina de 10 anos oriunda das filipinas para entrar em salas de chat. Como era necessário ligar a webcam para continuar na sala, assim para dar corpo e rosto a menina criou-se um modelo computacional dando a ilusão de estarem na presença de uma menina de carne e osso. Das

[75] Consultado, https://pplware.sapo.pt/informacao/cerca-de-1000-pedofilos-localizados-gracas-a-crianca-virtual/

informações cedidas pelos contactos que interagiam com a “sweetie” e cruzando com dados de fontes abertas como o Facebook ou google, foi possível identificar mais de 1000 homens. Todas as provas recolhidas pela organização que abarcam contactos de mais de 70 países, foram entregues a Interpol.

Marta Santos Pais, Representante Especial sobre a Violência contra as Crianças, Subsecretária-Geral da ONU alerta para a urgência do cumprimento das leis, leis que deverão ser severas para estes casos, já que a pedofilia é vista como proibida à base da lei internacional. O problema e a preocupação crescem com a globalização da Internet. Ela é cada vez mais acessível nestes países em desenvolvimento o que faz com que mais crianças sejam vítimas deste fenómeno. Mas se quando se fala em abuso sexual de menores, digamos que físico, parece que não se houve falar em negócio, as crianças são normalmente apanhadas no seio das famílias ou por conhecidos, sendo abusadas às escondidas. Neste caso, do abuso pela Web, na maior parte dos casos, é incentivado/obrigado pelos pais das próprias crianças, que vêm estes abusos como uma forma fácil de ganhar dinheiro.

Contudo, ainda muito está por legislar, é urgente criar políticas de combate pró-ativas que ajudem a apanhar em flagrantes estes homens, mas para isso é necessário que os Governos estejam abertos a criar infraestruturas para que tal venha a acontecer. A organização “Terre des Hommes” vem mostrar a facilidade de que é caçar os pedófilos da Internet, em apenas 2 meses conseguiram identificar 1000 homens simplesmente através de pesquisas em fontes livres da Internet. E se eles o conseguiram fazer, as autoridades poderão ir mais longe, condenando estas pessoas.

Em Portugal Criança virtual que localizou cerca de 1000 pedófilos não é aceite como prova.[76]

[76] Consultado em https://pplware.sapo.pt/informacao/sweetie-chumbada-como-prova-na-justica-portuguesa/

Segundo o advogado Luís Filipe Carvalho, “Está em causa um crime de abuso sexual de criança. Mas esse é um crime que pressupõe uma vítima. E aqui não há vítimas”. O advogado explica ainda que “mesmo que se entenda que se está perante um crime na forma tentada, continua a ser necessário que haja uma vítima”. Uma vez que a “Sweetie” é uma menina virtual, não pode ser considerada uma vítima pois seria “um crime impossível. É como dar um tiro a um morto.”

Ainda outro entrave para a nossa Justiça é o facto de a criança virtual ter sido colocada propositadamente na Internet para este efeito (caça de pedófilos), o que pode até ser considerado ilegal, uma vez que a Justiça Portuguesa não permite a figura do “agente provocador”. No entanto o jurista Paulo Saragoça da Matta afirma “Se era um papel passivo de ‘espera’ ou ‘emboscada’ pelos ‘avanços/ataques’ de pedófilos, nada de censurável jurídico-criminalmente pode inquinar a valia da prova obtida”. Mas, o jurista explica que se houver “um papel ativo de ‘provocação’”, então nesse caso a prova não poderá ser válida num processo criminal em Portugal.

Para tornar esta notícia ainda mais incrédula, o penalista Costa Andrade diz também que este método da “Terre des Hommes” deveria mesmo ser repudiado, pois segundo ele “Não é válido. Está mais próximo de um Estado totalitário”, e o que a menina virtual fez foi “detetar tendências”, sendo que os homens que a contactaram para fins sexuais não cometeram qualquer crime.

O penalista ainda adianta que “É muito discutível falar de pedofilia quando estamos perante um artefacto, uma boneca virtual”, e questiona que “Se a autoridade tributária puser uma boneca a anunciar na internet um esquema de fuga aos impostos, vamos acusar de crime fiscal quem disser que quer aderir?”

Contudo, o advogado Luis Filipe Carvalho diz que nada impede a Polícia Judiciária de usar a informação que a Interpol possa enviar sobre os portugueses pedófilos identificados: “Não há nada que obrigue os órgãos de polícia criminal

a abrir uma investigação, mas nada impede que se use essa identificação para realizar outras investigações".

O que retemos deste caso da "Sweetie" é que o recurso deste possível meio de investigação não se enquadra na figura de agente infiltrado apontado no ordenamento português, mesmo que estejam identificadas técnicas de infiltração.

2.7 MALWARE, AGENTE INFILTRADO DIGITAL

A utilização de um programa denominado de malware possibilita, genericamente, a observação e vigilância em tempo real bem como a cópia dos dados presentes no sistema informático. É discretamente instalado num sistema de processamento de dados, sem o conhecimento ou consentimento do utilizador, com o objetivo de colocar em perigo a confidencialidade daqueles dados, a sua integridade ou ainda a disponibilidade do sistema."[77]

Podemos encontrar várias modalidades de malware, sendo uma das mais conhecidas a que se dá pelo nome de "cavalo de Tróia". Apresenta-se como um ficheiro inofensivo, muitas vezes no correio eletrónico, levando a que o utilizador o ative através de um procedimento simples como seja "clicar nesse ficheiro". Dado esse passo, o malware cria uma "backdoor", ou seja, um acesso remoto não autorizado, ficando o sistema a mercê de quem controla o programa. [78]

Outra variante que podemos encontrar é o "spyware",[79] que, para além de enviar todos os dados do sistema, também consegue enviar informação sobre

[77] FILIOL, Eric, *Computer viruses: from theory to application*, Springer, 2005, p83

[78] RAMALHO, David Silva, *Métodos Ocultos de investigação Criminal em Ambiente Digital,* Edições Almedina, Maio 2017, p320

[79] ERBSCHLEO, Michael, *Trojans, Worms and Spyware* – A Computer Security Professional's Guide to Malicious Code, Elsevier Butterworth–Heinemann, 2005, p22

as teclas usadas pelo utilizador, muito útil para, nomeadamente, recolher "passwords".

Temos ainda as "LogicBombs", o qual é um malware que, depois de instalado, fica inativo a aguardar por um determinado acontecimento, podendo até ser programado para iniciar sua atividade numa hora pré-determinada. O seu efeito é igual aos demais malware já mencionados.

De referir, por último, uma modalidade um pouco mais agressiva, já que os seus efeitos vão mais além da simples recolha de dados informáticos, conseguindo afetar e destruir todos os programas do sistema. Existem duas formas destes malwares chegarem aos nossos aparelhos informáticos, seja através da interação humana, com o uso de uma "pen usb" – estando então na presença de um "Virus" – seja pela intranet, a que damos o nome de "Worms".[80]

Pelo acima exposto, estamos novamente perante um programa, algo não humano, como consideramos para a menina "Sweetie". No entanto, temos vozes na doutrina que apontam que seja possível utilizar este meio para a investigação, constituindo-se aqui a figura das buscas online ou até mesmo a figura do agente infiltrado digital.

Para Paulo Pinto de Albuquerque, este meio de obtenção de prova surge consagrado no artigo 15.º da LC, o qual prevê a possibilidade de "pesquisa em sistema informático", concluindo, contudo, pela sua inconstitucionalidade por intrusão na privacidade manifestamente desproporcional, "na medida em que a lei não coloca restrições relativamente ao conteúdo dos dados que podem ser pesquisados e, além disso, permite que o MP e o OPC ordenem a pesquisa de

[80] BOLDT, Martin, *Privacy-Invasive Software, Blekinge Institute of Technology*, 2010 p11

um sistema informático, sem o controlo prévio ou posterior da 'pesquisa' por um juiz.[81]

Não conseguimos encontrar eco nas palavras de Paulo Pinto de Albuquerque apenas pelo recurso à expressão "pesquisa em sistema informático", uma vez que tal diligência pode ser feita de forma presencial. Não esta expresso que tudo o que permita efetuar uma pesquisa seja aceite juridicamente. Logo, não enquadramos o recurso de um possível malware como um meio para efetuar a pesquisa no enquadramento da lei do cibercrime.

Ficamos assim mais próximos de Rita Castanheira Neves, que entende que a lei não oferece solução para a possibilidade de poderem ser recolhidos dados informáticos sem o conhecimento do visado.[82] Na mesma linha, João Conde Correia defende que a lei não oferece uma solução expressa, podendo ter duas interpretações. Por um lado, que as buscas online estão consagradas no artigo 15.º n.º 5 da LC (contudo, o que está aqui em causa é apenas a extensão online de uma pesquisa de dados informáticos em curso); por outro lado, a referência a "meios dispositivos e informáticos" do artigo 19.º n.º 2 da LC poderá ser interpretada como prevendo a possibilidade de realizar buscas online, possibilidade esta, limitada, contudo ao contexto das ações encobertas.[83]

Por fim, David Silva Ramalho entende estar no artigo 19.º n.º 2 da LC a consagração de um novo meio oculto de obtenção de prova "a utilização de malware", estando a sua utilização limitada ao contexto excecional das ações encobertas, por força da sua inserção sistemática. Entende o Autor que esta interpretação resulta do facto de os "meios e dispositivos informáticos" a que o

---

[81] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2011, p502

[82] NEVES, Rita Castanheira, op. Cit, p284

[83] CORREIA, João Conde, *Prova digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público, Ano 35, n.º 139, julho-setembro 2014, p42

artigo alude não se subsumirem a qualquer um dos meios de obtenção de prova previstos na legislação portuguesa. Deriva, de tal facto, a intenção do legislador de legitimar o recurso a um novo meio de obtenção de prova. Conclui, contudo, como Paulo Pinto de Albuquerque, pela existência de uma inconstitucionalidade por violação conjugada dos artigos 18.º n.º 2, 26.º n.º 2 e 32.º n.º 1 e 5 da CRP.[84]

Neste ponto, ficamos esclarecidos que o "malware" não se configura como um meio oculto de investigação – o dito agente infiltrado digital – nem se reconduz às buscas online, por falta de consagração legal no nosso ordenamento.

Vejamos agora se, ainda assim, é possível ser tido como um novo meio de obtenção de prova no nosso enquadramento legal.

O código de processo penal, no seu artigo n.º 125.º, estabelece o princípio da legalidade da prova, segundo o qual são admissíveis todas as provas que não forem proibidas por lei. Institui-se assim um sistema de prova livre ou de liberdade de prova. Não é, portanto, necessário que um meio de prova esteja expressamente previsto para que seja admissível.

Os meios de prova atípicos estão, naturalmente, subordinados aos limites constitucionais e legais de admissibilidade de prova. Os primeiros resultam do artigo 32.º n.º 8 da CRP, onde se estabelece a nulidade das provas obtidas sob tortura ou coação, obtidas com ofensa da integridade pessoal, da reserva da intimidade da vida priva, da inviolabilidade do domicílio e da correspondência ou das telecomunicações. Os limites legais, conformando o disposto na Constituição, resultam do artigo 126.º do CPP. Este artigo, nas alíneas n.º 1 e n.º 2, disciplina as provas absolutamente proibidas, isto é, as provas obtidas mediante tortura, coação e ofensa da integridade física ou moral da pessoa, que

[84] RAMALHO, David Silva, *op cit,* p349

nunca podem ser utilizadas por dizerem respeito a direitos que a Constituição consagra como invioláveis no seu artigo 25.º.

Por outro lado, o n.º 3 disciplina as provas relativamente proibidas, as quais dizem respeito a direitos que a Constituição admite serem limitados nos casos previstos na lei (artigos 26.º e 34.º n.º 3 e 4 CRP). Esta relatividade da proibição é diretamente extraível da Constituição quando, na segunda parte do n.º 8 do artigo 32.º, determina a nulidade das provas obtidas mediante intromissão abusiva na vida privada, no domicílio, na correspondência ou nas telecomunicações, devendo aqui ter-se por abusiva a intromissão quando efetuada fora dos casos previstos na lei e sem intervenção judicial ou quando em violação do princípio da proporcionalidade (18.º n.º 2 CRP). Admite-se, assim, *"A compressão de direitos constitucionais, numa lógica de proporcionalidade e exigido pelo próprio interesse do Estado no funcionamento da justiça penal."*

Terminamos este ponto invocando o entendimento de Paulo Pinto de Albuquerque, que refere que *"Quando o meio de obtenção de prova implicar um elevado grau de intrusão na privacidade do suspeito, ele deve ser previsto por uma lei expressa, salvo consentimento expresso e informado do visado"*.[85] Perante isto, resta-nos concluir dizendo que o "malware", também no campo de meio de obtenção de prova, deve ser excluído.

2.8 PROVA DIGITAL

Vigora, no sistema português, o princípio da imediação, o que significa que só em tribunal é que se produz realmente a "prova", tal como nos mostra o n.º 1 do artigo 355.º C.P.P. Apesar de, em linguagem corrente, se afirmar que os investigadores recolhem provas, o correto aqui é dizer que eles recolhem elementos de prova, o que significa que, apesar do todo o labor a montante do

[85]ALBUQUERQUE, Paulo Pinto de, *op cit*, p332

julgamento para a descoberta da verdade material, estas podem nunca chegar a constituírem-se como provas. A recolha de elementos de prova pretende, por um lado, determinar se alguém praticou ou não os factos qualificados como crime e, por outro, permitir ao tribunal que condene ou não aqueles culpados.[86]

No decurso da investigação criminal, é sobre os agentes que recai a obrigação da recolha de elementos de prova. Tais elementos destinam-se a descobrir os culpados da prática dos crimes e a permitir ao tribunal decidir do concreto grau de culpabilidade de quem é julgado, regendo-se pelos princípios constantes dos artigos 125.º e 127.º CPP, de acordo com os quais são admitidas todas as provas que não forem proibidas por lei, permitindo assim ao julgador formar a sua livre convicção sobre os factos controvertidos. Neste contexto, a prova recolhida em ambiente digital, a denominada "Prova Digital" não difere da recolhida em qualquer outro cenário de investigação.

Podemos afirmar que a prova digital não se diferencia das demais provas quanto ao seu valor probatório mas apenas pelo formato e ambiente em que se encontra, assim nos diz Silva Rodrigues como *"qualquer tipo de informação, com valor probatório, armazenada em repositório 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"*[87], e, também, Dias Ramos, que refere que a prova é *"informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta".*[88]

---

[86] VERDELHO, Pedro, *op cit* p117

[87] RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital (…),* Coimbra, 2009, pág. 722

[88] RAMOS, Armando Dias, *A Prova Digital em Processo Penal*, Chiado Editora, 1.º ed. Novembro 2014, pág. 86

Tendo presente que estamos num meio com características técnicas próprias e principalmente tendo em conta o seu cariz volátil, em que rapidamente as provas podem ser eliminadas pelo suspeito, o perito torna-se aqui numa peça chave na investigação e recolha de prova. Como perito, vai ajudar o agente da investigação a compreender determinados factos e preparar esses factos de modo a que eles sejam percetíveis em sede de julgamento.[89]

Para que a prova digital seja válida, ela tem que respeitar alguns princípios específicos de investigação forense, para além dos que estão consagrados no código de processo penal. Assim, e como forma de garantir a integridade da prova obtida durante a sua recolha, armazenamento e tratamento (como consagra o princípio de não alteração da prova no ato de recolha) ao investigador também é pedido que não contamine os sistemas sob investigação por recurso dos meios utlizados na investigação. Juntamos aqui ainda o princípio da especialização forense impede que o perito, por meio dos seus conhecimentos, corrompa a prova por via de um inadequado manuseamento, fazendo com que a prova seja tida como inválida para o processo.[90]

Um outro princípio de que consideramos de grande importância é a *garantia de documentação em todas as fases processuais,* que estabelece que uma investigação forense terá por base a integridade da cadeia de controlo. Para tal, é necessária a apresentação de documentação em todas as fases. Este princípio acarreta uma necessidade de se ver garantido um controlo reforçado dos investigadores. Apenas através da *"reversão dinâmica"* será possível repetir a prova, cabendo aos agentes competentes a tarefa de descrever da forma mais detalhada possível os resultados obtidos na fase anterior.[91]

---

[89] VERDELHO, Pedro, *op. cit,* p120

[90] RODRIGUES, Benjamim Silva, *op cit* , pág726

[91] RODRIGUES, Benjamim Silva, *ibidem*, pág728

Tendo apurado, até ao momento, que a prova obtida em ambiente digital – exceto pelas suas características técnicas – não difere das provas tradicionais, resta apurar se temos então uma legislação dedicada para este tipo de prova.

Começamos pelo Código Processo Penal, e pelos artigos 189.º e 190.º, que remetem para os artigos 187.º e 188.º (o mesmo regime que é aplicável às escutas telefónicas), ficando, ambas as provas, sujeitas ao mesmo regime, apesar de ter acrescentado "mesmo que se encontrem guardados em suporte digital". Seguimos aqui o mesmo entendimento de Costa Andrade, no sentido em que o artigo 189º engloba várias realidades distintas, necessitadas de tutela e exigências distintas, causando incerteza e insegurança jurídicas e dificultando o controlo, por parte das instâncias formais competentes. Partilhamos da visão do mesmo autor, pois, ao integrar o *e-mail* guardado no computador no regime das escutas telefónicas, a investigação criminal é posta em causa, visto que passa a garantir ao meio informático um regime mais estável do que ao regime das escutas, fazendo deste artigo a *"casa dos horrores hermenêuticos".*[92]

Como forma de transpor para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15/3, é adotada a Lei n.º 32/2008, de 17/7, uma lei extravagante, visando regular a conservação e transmissão dos dados de tráfego e localização, e os dados relevantes para a identificação do utilizador, garantindo a investigação e futura repressão de crimes graves. Na existência de um catálogo restritivo de crimes, a transmissão de tais dados depende de despacho fundamentado do juiz de instrução criminal, se este os determinar indispensáveis para a descoberta da verdade, sendo impossível ou bastante difícil de a alcançar sem tais provas. Para tal, o artigo 9.º, n.ºs 1 e 2 da dita Lei defendem a necessidade de serem respeitados os princípios da adequação, da necessidade e da proporcionalidade. O número 3 do dito artigo restringe ainda esses dados transmissíveis apenas aos referentes ao suspeito/arguido, ao suspeito de receber ou transmitir as mensagens em

[92] ANDRADE, Manuel da Costa, *"Bruscamente no verão passado",* Coimbra Editora, 2009*.,* p185

causa, ou à própria vítima, mediante o seu consentimento.

Por fim, quanto à legislação existente, temos o diploma da lei do cibercrime 109/2009 que adapta a decisão 2005/222/JAI do conselho de 24/2, substituindo a lei da criminalidade informática de 1991. Em matéria de disposições penais materiais, o legislador excluiu o catálogo de crimes informáticos do Código Penal, mantendo o catálogo de crimes de Devassa por meio de informática e de Burla Informática, expostos nos artigos 193.º e 194.º, respetivamente. A Lei do Cibercrime engloba entre os artigos 3.º e 8.º, os crimes de Falsidade Informática, dano relativo a programa ou outros dados informáticos, Sabotagem Informática, Acesso Ilegítimo, Interceção Ilegítima, e Reprodução Ilegítima de programa protegido. Apesar de ser "*do Cibercrime*", esta lei engloba no seu regime os crimes informáticos *stricto sensu*, já então previstos; aqueles que sejam cometidos por meio de um sistema informático; e aqueles em que seja relevante aceder a métodos de escolha e prova em suporte eletrónico (artigo 11.º, n.º 1).

2.9 AGENTE INFILTRADO DIGITAL

Vamos agora verificar os pressupostos do agente infiltrado no meio digital comparando com os pressupostos do agente infiltrado tradicional, ou seja, pertencente ao meio físico.

Qual pode ser o risco de exposição que o nosso agente na rede cibernética pode ter? Sabemos que, no mundo físico, o agente poderá integrar a estrutura criminosa, ficando exposto a um enorme perigo e mesmo com grande risco para a sua própria vida. No ambiente digital, esse risco desaparece por completo, tendo em conta que não existe uma interação física, passando-se tudo meramente com um interlocutor num meio como por exemplo computador, tablet, ou um smartphone. A falta de contacto, característica do mundo virtual, possibilita que a aparência dos sujeitos, incluindo a do agente, não seja possível de identificar, bem como facilmente ser possível ocultar a sua real localização. Sabemos que o agente infiltrado atua com a ocultação da sua qualidade e

identidade, reconduzindo no ambiente digital a um perfil falso, e disso temos a internet cheia, e até há utilizadores que entram na rede com recurso ao roubo do perfil de terceiro. Esta prática, de perfil falso em ambiente digital, que não encontra sanção no mundo jurídico, faz com que seja natural, criando uma enorme dificuldade de identificar os utilizadores na rede.

Partindo do que acabamos de expor, verificamos que o agente pode entrar na rede com um perfil falso, para ocultar a sua identidade, sem ter a necessidade de um despacho do mistério público, e este ponto parece-nos um pouco preocupante. Apontamos dois motivos para a nossa preocupação: num primeiro momento, como vamos ter a certeza que determinado perfil corresponde a um agente infiltrado, caso venha a ser criado um processo penal no futuro, e ainda, como pode depois ser aplicado o princípio do contraditório se não se sabe contra quem pode ser feito por não existir prova que aquele perfil era realmente o de um agente; num segundo momento, uma questão que afeta o nosso agente em ambiente virtual é a de ele não ser apenas um só, mas podemos estar na presença de vários agentes que utilizam apenas um perfil dando a entender que é uma única pessoa. Esta é uma técnica muito útil quando há necessidade de uma vigilância permanente. O agente pode ainda interagir ou não com os investigados dado que pode entrar numa sala pública de um chat e ficar apenas a ver as conversas que estão a ser tidas nesse site pelos diversos utilizadores, mantendo uma atitude de simples espectador.

Uma questão que já era tida como ponto de preocupação quando estamos na presença do agente infiltrado em meio não digital, é a relativa ao tema “provocação”. Ficou patente que, no nosso ordenamento, tal atitude não é aceite, embora o Professor Rui Pereira, em certos casos pontuais, admita que possa ser aceitável uma ligeira provocação. Vamos criar dois cenários para descrever como pode esta questão ser abordada na perspetiva cibernética. Num primeiro cenário, o agente cumpre legalmente os requisitos para se proceder ao recurso deste método oculto de investigação. Ao entrar numa sala pública que, de antemão, se sabe ser frequentada por pedófilos, de certeza que se não tiver uma

atitude ativa não irá criar qualquer contato, e se aspira a ser convidado para meios mais privados, as suas possibilidades serão com um grau elevado de certeza praticamente nulas. Encontramos eco na solução dos nossos vizinhos espanhóis ao aceitar que o agente exerça de forma controlada alguma provocação, como seja a de fornecer fotografias de menores para aumentar o sucesso da investigação. Outro cenário que podemos imaginar é o da operação de infiltração ter vários agentes infiltrados e um ou até mais provocarem de formar a encaminhar os suspeitos para os outros agentes. Nesta situação, os provocadores, que até podem nem ser agentes e atuar de forma consertada, eles próprios recorrem à ocultação que a rede permite, evitando surgir em qualquer processo, não sendo assim possível criar uma ligação entre agentes infiltrados e a provocação que ocorreu.

Tradicionalmente, o agente infiltrado físico envolve-se num meio também ele físico. No que diz respeito ao agente digital, ele infiltra-se com recurso ao meio virtual e, conforme o desenvolvimento da investigação, pode manter-se nesse mundo ou interagir depois no meio físico também. Ao utilizar exclusivamente meios informáticos, ele atua em chats, fóruns, websites ou blogs e fica sujeito tanto à lei do cibercrime como à lei do regime jurídico das ações encobertas. O principal meio de comunicação é feito através da escrita, que, se for devidamente registada, pode servir de prova, neste caso prova digital. E ainda temos outros documentos, como por exemplo fotografias que sejam cedidas pelo suspeito, as quais terão apenas de respeitar os procedimentos legais para que venham a permitir que o tribunal as possa utilizar esses elementos como qualquer outro meio de prova legal. Se o agente deixar de atuar no meio digital, fica abrangido apenas pelo RJAE, como um agente infiltrado tradicional do mundo físico.

Se os meios ao dispor da investigação criminal têm evoluído, também se regista que os agentes do crime não ficaram parados no tempo. A internet, como a maioria dos utilizadores conhece, é apenas a ponto do iceberg de toda a rede; daí ter surgido o termo “Darkweb”, para a parte escondida da maioria, ou seja, a

parte imersa. Esta foi inicialmente projetada para assegurar comunicações militares norte americanas mais seguras em caso de falha da rede normal. O que se conhece, em termos gerais, é que, para além da rede que qualquer utilizador usa, existe outras em que são necessários alguns conhecimentos técnicos, o recurso de programas próprios, ou fazer prova para poder aceder a determinados sites. Assim, a criminalidade nestes meandros desenvolve-se sem que possa ser aplicado um controlo efetivo; a juntar a este facto temos a disseminação de moedas virtuais, como as "bitcoin" de grande valor monetário, e de difícil localização ou possibilidade de rastear as transações com que são realizadas através deste tipo de moeda. Para tentar combater a cibercriminalidade, diz-nos o inspetor Rogério Bravo que todo o dispositivo informático deixa uma pegada digital no ciberespaço que pode ser investigada nos diversos dispositivos eletrónicos que são os dados de tráfego e que devem ser tidos como prova digital.[93]

Como todos sabemos, a velocidade com que se realizam as operações com os meios informáticos são cada vez mais rápidas, e o que num determinado momento existe de informação num terminal informático pode rapidamente desaparecer. Impõe-se então que aos agentes seja facultado o apoio necessário para salvaguardar os dados de tráfego e a possibilidade de rapidamente poderem atuar na recolha de dados para evitar que sejam destruídos.

Já apontamos para a possível falta de despacho judicial sobre o perfil que o agente infiltrado digital irá utilizar para proceder a sua investigação. Acreditamos que deveria haver um despacho completo em que estaria registado quais são os utilizadores admissíveis assim como quais os sistemas informáticos a partir dos quais poderão ser realizadas as ações encobertas. Também temos presente que devem ser elencados os atos autorizados e não autorizados para

93 http://www.academia.edu/4691991/DOS_VEST%C3%8DGIOS_EM_AMBIENTE_DIGITAL_%C3%80_PROVA_DIGITAL_COMO_INTELLIGENCE

evitar quaisquer tipos de abusos ou ainda para poder delimitar a forma como pode contactar com os possíveis suspeitos sem que entre no campo da provocação. Por fim, nesse despacho poderia constar quais os websites, chats ou fóruns que estaria autorizado a frequentar e com quem interagir.

Quanto ao prazo de duração deste tipo oculto de investigação com recurso ao agente infiltrado digital, este deve ter um prazo estabelecido para que os meios sobre os quais recaem a investigação não fiquem reféns das autoridades.

3 CAPÍTULO III AS ENTREVISTAS E RESPETIVA ANÁLISE

A entrevista trata-se de um tipo de instrumento que "permite explorar um domínio e aprofundar o seu conhecimento através da inquirição presencial a um ou mais indivíduos. Os seus conteúdos são mais ricos em informação". Basicamente, uma entrevista é "um conjunto de perguntas (designado por guião), que são respondidas necessariamente por via oral".[94]

Foram realizadas entrevistas com o intuito de determinar o impacto do mundo cibernético tem em Portugal e analisar as preocupações dos institutos, que mais perto lidam com este meio, sobre a segurança para os utilizadores.

Contactamos o Gabinete Nacional de Segurança que tem sobre a sua alçada o centro nacional de cibersegurança e este com a missão de contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que,

[94] SARMENTO, Manuela, *Metodologia científica para a elaboração, escrita e apresentação de Teses,* Universidade Lusíada Editora, Lisboa 2013, p30

face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

O outro instituto visado nas nossas entrevistas foi o Centro Nacional de Ciberdefesa que tem no âmbito da ciberdefesa, a missão de coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas.

Por fim entrevistamos um inspetor da Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica (UNC3T) tem as seguintes competências:

a) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na Lei nº 109/2009, de 15 de setembro;

b) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos,

De entro outras que podem ser consultadas no seguinte endereço https://www.policiajudiciaria.pt/unc3t/

Quanto à preparação das entrevistas, foram seguidos os princípios definidos por Marconi & Lakatos[95] em que, na construção da entrevista foi elaborado um guião inicial, revisto pelo Orientador da presente investigação. Os guiões finais podem ser consultados no anexo A, a suas transcrições no anexo B

[95] MARCONI, Marina de Andrade, LAKATOS, Eva Maria*, Fundamentos de Metodologia Científica,* 5ª ed, Editora Atlas, São Paulo 2003

No que diz respeito à classificação apresentada por Sarmento, as entrevistas aplicadas no presente trabalho classificam-se como presenciais, quanto ao modo e individuais, e quanto ao número de pessoas

As instituições escolhidas estão ligadas pelo mundo do ciberespaço e não estão como tal, propensas numa espectativa de recurso do agente infiltrado digital, este como tivemos oportunidade de estudar cabe a investigação criminal sob o controlo da polícia judiciaria. Mas entendemos que pela interação das instituições em causa pode existir uma relação para que seja utilizado ou não o agente que estudamos.

A primeira questão posta aos nossos entrevistados era em saber quais as preocupações presentes, o tanto a cibersegurança como a ciberdefesa têm o seu foco na rede e no cumprimento de protocolo internacionais de segurança. Estes procedimentos permitem que a informação que circula na rede esteja sob maior proteção, que é o ponto em que a ciberdefesa tem os olhos postos. Se houver uma boa segurança leva que os crimes a unidade de cibercrime se dedica, sejam menores.

A pergunta seguinte é de saber das ameaças que vem do ciberespaço se temos alguma que se destaque. E novamente para a Cibersegurança e Ciberdefesa o problema não esta propriamente dentro da rede mais sim fora, por falta de recursos humanos para fazer face as ameaças. Para a unidade de cibercrime é dedicado a todas as ameaças cibernéticas, sejam crimes informáticos próprios (que nascem e morrem dentro do ciberespaço) ou impróprios (mesmo não usando meios informáticos estariam presente na mesma.)

A pergunta terceira pergunta foca-se em clarificar se temos uma proatividade na procura de incidentes na rede ou se há uma certa passividade. Todos os entrevistados alegaram que obtêm o conhecimento por outras identidades ou por denuncias, fazem monotorização de âmbito preventivo. Quanto a executar algum tipo de investigação esta cinge a área da respetiva

atuação, caso obtenha informações de situações que não lhe cabe em competência transmitem a quem é devida.

Como resolvem as ameaças que enfrentam, cada instituição tem a sua posição. Para Cibersegurança é através de ações de formação que tende a fazer face, por considerar que o capital humano é muito importante no combate a insegurança da rede. A Ciberdefesa avalia os ataques que sofre e tende a resolver as situações que se lhe apresentam, disponibilizando depois as soluções aos sistemas para garantir um melhor segurança. Para a unidade do cibercrime não chegam os meios técnicos, sem os meios humanos adequados também é complicado enfrentar a criminalidade digital, como é para a criminalidade em geral.

Um ponto que não podíamos deixar de fora era saber o que pensam os nossos entrevistados sobre o tema de cooperação. Aqui todos eles foram perentórios com um grande sim, tem de haver cooperação e sim ela existe.

Continuando com a questão seguinte sobre a realização de exercícios para fomentar essa cooperação, também aqui foram unanimes nas respostas, ressalvando que cada um tem de ter os exercícios adaptados as suas próprias necessidades.

Também procuramos inteirar para quem tem um papel na segurança em geral do ciberespaço, a opinião que têm do publico em geral. Aqui mais uma vez a opinião foi no mesmo sentido, em que há algum publico que tem noção de a rede ter alguma insegura, mas de modo geral não há uma grande preocupação.

Como forma de aumentar a segurança, visando os comuns utilizadores, o que fazem as nossas instituições entrevistadas. A cibersegurança tem ações de formação e promove muitas conferencias pelo país, a ciberdefesa como vertente mais militar tem o enfoque nos seus utilizadores em que lhes seja facultado regras de utilização para ter um elevado índice de segurança. A unidade de cibercrime as suas ações de formação são mais de consumo interno.

No tema sobre a legislação ser suficiente e adequada apenas o Sr. Inspetor Rogério Bravo alertou para um meio que esta em constante mutação e pela velocidade que opera, será difícil que a lei consiga acompanhar.

Sobre se Portugal esta a par com os restantes parceiros da Europa, também aqui temos um consenso, temos qualidade sem sombra de duvida, mas o ratio de meios humanos confrontado com outras realidades é muito baixa.

Concluímos as nossas entrevistas colocando duas perguntas exclusivas ao Sr. inspetor da judiciaria sobre o agente infiltrado.

A primeira foi apurar se o meio de investigação em causa é um meio banal ou excecional como diz o Professor Guedes Valente. Para o nosso entrevistado é claro que estamos perante um meio excecional que só deve ser utilizado para casos graves. Por fim se o quadro legal é condizente com a figura do agente infiltrado remete para o que já tinha frisado, de momento sim, mas a evolução é tão rápida que a lei não acompanha da mesma forma.

4 CONSIDERAÇÕES FINAIS

A sociedade esta constantemente em mutação, esta situação não é nova nem exclusiva dos tempos modernos, pertence a história da humanidade. Esta evolução vem de mãos dadas com o direito, "Ubi homo ibi societas; ubi societas, ibi jus", assim referia Ulpiano no "Corpus Iuris Civilis", ou seja: onde está o Homem, há sociedade; onde há sociedade há direito. Para que esta máxima tenha sentido, o direito tem de acompanhar as novas tendências, os novos comportamento, as novas situações da vida da sociedade. A sociedade digital fervilha com novos acontecimentos a uma velocidade estonteante, ao ponto de alguns serem efémeros. O direito por norma tende a cimentar-se de forma lenta, e como tal não acompanha os acontecimentos dos tempos modernos. Para colmatar esta lacuna a solução encontrada é em adaptar figuras jurídicas já existentes convertendo-as as necessidades atuais. Interessa saber então, se estamos perante a melhor solução para a situação em concreto.

A nossa dissertação versa sobre a figura do agente infiltrado em ambiente digital, e procura saber se a adaptação de uma figura jurídica do mundo físico esta de acordo com os princípios do Direito instituído.

Para conseguir chegar a uma conclusão iniciamos o nosso estudo tendo por base o regulamento jurídico das ações encobertas, e assim identificamos quem é o agente infiltrado no nosso ordenamento. A doutrina não é consensual, muito por culpa da incerteza gerada pelo termo “terceiro “, o que leva alguns autores a prolongar o vínculo do agente a qualquer pessoa, seja polícia ou civil. Tomamos uma posição clara e sustentada, o agente infiltrado não pode sair da esfera policial, ou seja, só os OPC’s ou elementos das forças de segurança lhe poderão vestir a pele. Esta posição abrange também quando o agente pertence ao mundo digital.

Temos a disposição da investigação criminal diversos meios ocultos de obtenção de prova. Abordamos este tema para demonstrar a relação entre eles e deixar presente que apesar de todos colidirem com direitos fundamentais, não

tem todos a mesma intensidade, aqui realçamos a falta de uma ordenação dos meios, que permitiria o correto respeito pelo princípio da subsidiariedade.

A conjugação do RJAE com a lei do cibercrime não veio a alargar que determinados meios ocultos como o que foi utilizado no caso “Sweetie” seja enquadrado como agentes infiltrados. Também o “malware” ou programas informáticos similares foram excluídos como agentes, isto resulta que a lei do cibercrime apenas prolongou o recurso do agente para o meio digital sem alterar a sua forma, ou seja tem de ser uma pessoa física, mas agora nada impede que seja apenas um individuo, podemos estar perante uma equipa de investigadores.

Sobre a recolha de elementos de prova, o agente quer físico quer virtual pode ter acesso ao mesmo tipo de provas. É verdade que o agente no meio digital vai ter um maior contato com provas digitais, mas também terá acesso as provas tradicionais, porque ele pode pelo decurso da investigação passar do mundo físico para o digital e vice-versa. O importante é que seja respeitado os procedimentos na recolha dos elementos que venham a servir de prova pelo tribunal.

O ponto mais critico do nosso estudo é sobre figura do agente provocador, em que o fim atingido não é a descoberta da verdade, mas sim instigar o crime, como tal esta figura não é aceite no ordenamento português. O ciberespaço proporciona duas características bem vincadas, a falta de fronteiras que criar diversos obstáculos a aplicação do direito interno, e ainda o anonimato muitas vezes sobre o manto de perfis falsos.

Este comportamento joga tanto para o lado da investigação criminal como para o mundo do cibercrime. O agente ao abrigo de um perfil falso, que pode ser requerido judicialmente, mas também pode não o solicitar, e temos assim um utilizador na rede como outro qualquer, agindo ou não de forma concerta com outros agentes, provocando instigando sem limites, porque joga com as regras do ciberespaço e não com as regras legais.

O professor Rui Pereira deixa a porta da provocação ligeira para certos casos aberta, quando fala do agente infiltrado físico. O meio digital não se compadece com inatividade, necessita de impulsos, isso acontece por exemplo nas salas de chat, onde se quer investigar crimes de ordem sexual, o nosso agente utilizador na rede não pode ter o mesmo comportamento que tem no ambiente não digital, porque a mera presença física já por si pode criar interesse em ser contactado, enquanto no meio virtual tem que provocar esse contacto o que se confundo com provocar o crime. O ordenamento espanhol autoriza que o agente entregue de fotos de crianças quando investiga crime de pedofilia.

Concluímos que a adaptação do agente infiltrado digital tem o mesmo valor jurídico que o agente em ambiente físico. Não negamos que deveria estar elencado, por um despacho judicial quais os meios ao dispor do agente assim como quais os limites da sua atuação, e ainda os endereços, os fóruns, as salas de chat autorizado a frequentar, por fim o recurso do perfil falso só mediante despacho judicial como sucede para o agente do mundo físico.

Terminamos completando com as respostas dos nossos entrevistados. Ficou claro que o ciberespaço tem diferentes abordagens possíveis, e a mais importante é a cooperação entre as instituições, que ao avaliar as ameaças que sofrem podem transmitir às outras instituições em tempo oportuno para se protegerem também. A formação e os recursos humanos foram outro ponto de destaque, transversal a todos os nossos entrevistados.

Se tivermos um nível de segurança elevado proporcionado pelos diversos quadrantes, haverá uma menor criminalidade em geral, e assim também menos hipótese de recurso de um meio tão excecional de obtenção de prova, como é o agente infiltrado.

Anexo A

Guião das Entrevistas

Guião da entrevista realizada:

Gabinete Nacional de Segurança e Centro Nacional de Cibersegurança

I Identificação da entrevista

1 Data da Entrevista:

2 Hora da Entrevista:

3 Identificação do entrevistado

4 Profissão do Entrevistado

II Questões:

1 - Quais são as preocupações prioritárias do (GNS / CNS)?

2 - Quais as principais ameaças que o (GNS / CNS) considera mais relevantes?

3 – De que forma adquirem conhecimento das ameaças, através da monotorização ou de investigação?

4 Quais são as atividades que o (GNS / CNS) desencadeia para solucionar as ameaças?

5 - O problema da Segurança é hoje em dia Global, o (GNS / CNS) considera a cooperação essencial entre as instituições tanto a nível interno com a nível externo?

6 - Como forma de fomentar essa cooperação o (GNS / CNS) considera a realização de exercícios de treino proveitosos nesse sentido?

7- A segurança é de todos, o (GNS / CNS) considera que o publico em geral tem consciência sobre o tema?

8 - Como forma de melhorar a segurança, o (GNS / CNS) desenvolve algum programa de formação e respetiva divulgação ao público?

9 - Considera a Legislação atual suficiente e adequada para o desempenho das funções do (GNS / CNS)?

10 - Considera que Portugal esta a par com os restantes países da união europeia ou ainda existem atrasos?

Guião da entrevista realizada:

Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica

I Identificação da entrevista

1 Data da Entrevista:

2 Hora da Entrevista:

3 Identificação do entrevistado

4 Profissão do Entrevistado

II Questões:

1 – Tendo em conta os recursos disponíveis, quais são as preocupações prioritárias da Polícia Judiciaria no combate ao cibercrime?

2 – Considera a o leque dos crimes elencados na lei do cibercrime que é condizente com os delitos praticados no ciberespaço?

3 – De que forma adquirem conhecimento dos crimes, através da monotorização ou de investigação?

4 A Polícia Judiciaria Tem meios técnicos e humanos adequados a realidade para o combate da cibercriminalidade?

5 - O problema do cibercrime é hoje em dia Global, a Polícia Judiciaria considera a cooperação essencial entre as instituições tanto a nível interno com a nível externo?

6 - Como forma de fomentar essa cooperação, considera a realização de exercícios de treino proveitosos nesse sentido?

7- A segurança é um bem de todos, considera que o público em geral tem consciência sobre o tema cibercrime?

8 - Como forma de reduzir a cibercriminalidade, a Polícia Judiciaria desenvolve algum programa de formação e respetiva divulgação ao público?

9 - Considera a Legislação atual suficiente e adequada para o desempenho das funções Polícia Judiciaria sobre o cibercrime?

10 - Considera que Portugal esta a par com os restantes países da união europeia ou ainda existem atrasos no combate ao cibercrime?

11 - O agente infiltrado digital é um meio oculto de investigação de último recuso ou de primeira linha?

12 - Considera que o atual quadro jurídico-penal que regula o instituto do agente infiltrado no meio digital é apropriado ou carece de alguma alteração profunda?

Anexo B

Transcrição das entrevistas

Entrevista realizada ao Sr. Diretor do GNS Almirante Gameiro Marques

1 - Quais são as preocupações prioritárias do Gabinete nacional de segurança?

Entrevista Nº1 da revista AMA Garantir a diretiva SRI segurança redes e sistemas informação, transposição da lei nacional maio de 2018, e dar origem à lei de cyber segurança. Transposição deverá ser feita de forma correta. Receber até ser publicada, contributos de todas as entidades públicas e privadas que vão trabalhar com a lei, para Portugal não estar sujeito a multas da União Europeia. É um compromisso internacional. Garantir que o conselho superior de segurança cyber espaço, criado agosto pelo conselho de ministros em 2017, cumpra cabalmente a sua função. Execução da estratégia, coordenada e coerente. Dotar o centro nacional cyber segurança em geral, departamento de operações em particular, onde funciona o CERT PT, computer emergency response team, com meios humanos, materiais e financeiros necessários para cumprir a missão.

1 - Quais são as preocupações prioritárias do Gabinete nacional de segurança?

O dinamismo da economia nacional, motor na área de tecnologias de informação, a procura de pessoas na área civil maior que a oferta. Poucos recursos humanos, formados e treinados. Quando isso acontece estão pouco tempo nessas funções, não se torna competitivo para angariar recursos humanos. Sem meios humanos devidamente formados e treinados a tarefa torna-se difícil. Esta é uma especifica do centro nacional de cyber segurança português. Apesar de na administração pública sermos competitivos em termos salariais no privado não o somos, sobretudo para indivíduos seniores. Depois existe a ameaça inerente de estarmos no cyber espaço. Todos os dias surgem ameaças diferentes. Não há patch antivírus contra. Mas a procura de recursos humanos qualificados ser maior que a oferta é a maior ameaça.

3 – De que forma adquirem conhecimento das ameaças, através da monotorização ou de investigação?

Fazemos parte da rede SEA Search europeia e nacional. Também fazemos, desde agosto, parte duma rede global FIRST, fórum global sea search. Globalmente com a partilha de informação, nacional e internacional, rapidamente adquirimos conhecimento que nos permite ser tentativamente preventivos e não reativos. Outro aspeto prende-se com o facto de tentar sensibilizar as pessoas e garantir que a confiança seja ganha. Assim partilham a informação com maior facilidade. É uma conjugação entre trabalhar em rede e garantir que a relação entre as entidades dessa rede ganhe robustez nessa confiança.

4 - Quais são as atividades que o Gabinete nacional de segurança desencadeia para solucionar as ameaças?

“A melhor forma de estarmos protegidos é estarmos preparados”. Prevenção e preparação das pessoas. Isto com formação sólida, na Nacional Defense University, em Thalin da Nato, Marschal Center. Desenvolvemos em conjunto com parceiros públicos, respostas pré planeadas baseadas num conjunto de cenários previsíveis, que quando detetada a ameaça se definem procedimentos em função dum cenário. Objetivo; diminuir o tempo de resposta. Antes de surgirem, fazemos esta prevenção, depois de surgirem, tentamos rapidamente perceber que procedimentos a fazer para estancar o problema, a ameaça, como aconteceu o “PHATIA” e tentar solucionar os serviços afetados e repor o mais rapidamente possível. Monitorizar o cyber espaço de interesse, o “PANORAMA”.

5 - O problema da Segurança é hoje em dia Global, o Gabinete nacional de segurança considera a cooperação essencial entre as instituições tanto a nível interno com a nível externo?

Necessidade de liderança em colaborar, eficaz e notória. Quem deve decidir deverá ser quem tem maior informação para que a ameaça tenha o menor impacto possível.

6 - Como forma de fomentar essa cooperação o Gabinete nacional de segurança considera a realização de exercícios de treino proveitosos nesse sentido?

Sim temos o CMX 2017 a decorrer com elementos do centro envolvidos. CYBER COLISION e PERSEUS para futuras participações.

7- A segurança é de todos, o Gabinete nacional de segurança considera que o publico em geral tem consciência sobre o tema?

O público em geral tem mais conhecimento nos dias de hoje que anteriormente. Estes assuntos são mediáticos e bastante falados na comunicação social. AON – entidade internacional de gestão de risco. Produz relatórios de empresas para se perceber quais os maiores riscos. Em 2015 assuntos sobre o cyber risco entrou para o 9º lugar, este ano está em 5º lugar. Já existe conhecimento sobre este assunto. Maior consciência sobre o risco desta ameaça.

8 - Como forma de melhorar a segurança, o Gabinete nacional de segurança desenvolve algum programa de formação e respetiva divulgação ao público?

Regularmente, semanalmente, damos conferências, painéis, sobre este tema. Fomentar a consciência das pessoas que este assunto tem de estar em cima da mesa e que não acontece só aos outros.

9 - Considera a Legislação atual suficiente e adequada para o desempenho das funções do Gabinete nacional de segurança?

Quando for promulgada ou publicada a lei cyber segurança e o subsequente regulamento da lei as coisas começarão a ficar mais consolidadas. Já temos a lei de cyber crime, trabalhamos já com a polícia judiciária. Com a lei de cyber segurança tal como está concebida vamos ficar com uma “Frame Work” adequada para execução.

10 - Considera que Portugal esta a par com os restantes países da união europeia ou ainda existem atrasos?

A posição de Portugal no índice ITU não reflete a realidade. Mas o caminho é longo e reitero ainda a maior ameaça; recursos humanos! Talvez estejamos a par com a média dos países da união europeia.

Entrevista realizada ao Chefe adjunto do CNC, CMT Camara Assunção

1 - Quais são as preocupações prioritárias do Centro de Ciberdefesa?

O centro de ciberdefesa como vertente ligada as forças armadas preocupa-se com todos os ataques a sua rede de infraestrutura

2 - Quais as principais ameaças que o Centro de Ciberdefesa considera mais relevantes?

Diria que são para além que qualquer instituição pode sofrer, são o que podem estar ligados com a ciberespionagem.

3- De que forma adquirem conhecimento das ameaças, através da monotorização ou de investigação?

Sistema faz a recolha de 600 a 700 eventos por segundo. É muita informação, ao olho humano não dá para ler toda aquela informação e correlacionar informação uma com a outra, isto são os sistemas de monitorização. É evidente que alguma coisa pode falhar. A investigação dentro da Cyber defesa e Forças Armadas serve para adquirir capacidade forense para analisar sistemas afetados, determinar a origem de forças A B, ou C. Posso saber determinado endereço IP que está a atacar a firewall com ataque de DIN service e esse endereço possa ser ponto de saída. Já ouviu falar em Deep web e Dark web por baixo das camadas sai da deep web desse ponto de saída. Uma das coisas a saber é a origem, como a ameaça começou e como funciona. O malware para transformar máquina como zombies com o vírus introduzido, tipo bote net com milhões de equipamentos. O software malicioso está sempre á espera de informação. Se descobrirmos que alguma informação for descoberta, extraída, convém alterar o plano inicial.

4 Quais são as atividades que o Centro de Ciberdefesa desencadeia para solucionar as ameaças?

Temos um Sítio de resposta a incidentes, deteção, mitigação e vulnerabilidade. Estudo para detetar o impacto da ameaça. Arranjar uma solução para todos os sistemas. Centro de resposta de incidentes de segurança informática. Na Questão se temos investigação criminal cyber crime? Não é da competência da cyber defesa das forças armadas a análise forense para apresentar provas em tribunal. Polícia judiciaria militar PJM e Judiciária civil realizam peritagens quando necessário, para determinar a origem e o que a ameaça faz. De seguida mitigar essa mesma ameaça.

5 - O problema da Segurança é hoje em dia Global, o Centro de Ciberdefesa considera a cooperação essencial entre as instituições tanto a nível interno com a nível externo?

Cooperação entre instituições é essencial, entre a cyber defesa e forças armadas, rede CSIRT computer security incidente response teams. Rede entre vários organismos que discutem esses incidentes informáticos, parte militar e civil. A rede nacional funciona com a partilha de informação entre organismos. Prevenir, com essa partilha de informação, é muito importante.

6 - Como forma de fomentar essa cooperação o Centro de Ciberdefesa considera a realização de exercícios de treino proveitosos nesse sentido?

Existe o Cyber Perseu, do Exército. Exercício Nato, o Cyber Colision, maior evento em termos de cyber segurança, focado na partilha de informação entre forças. A Marinha nunca participou no Cyber Perseu, mas não está excluída uma futura participação. É bastante proveitoso esse treino conjunto porque é o mais perto da realidade. Criar procedimentos globais entre países e instituições.

7- A segurança é de todos, o Centro de Ciberdefesa considera que o publico em geral tem consciência sobre o tema?

As pessoas não estão conscientes com este assunto. Sentimento de desinteresse, são descuidados. A tendência é para melhorar, mas muito lentamente, dá tempo para hackers se prepararem e evoluir. O elo mais fraco são as pessoas. A interface homem / máquina tem de melhorar para ser mais eficaz.

8 - Como forma de melhorar a segurança, o Centro de Ciberdefesa desenvolve algum programa de formação e respetiva divulgação ao público?

-Os Utilizadores que operam sistemas de informação nas forças armadas muitas vezes descuidam as com regras básicas, apesar de alertados. Estando a sair fora da responsabilidade individual permite erros e provoca incidentes prejudiciais á segurança do individuo ou sistema.

9 - Considera a Legislação atual suficiente e adequada para o desempenho das funções do Centro de Ciberdefesa?

Não preciso de legislação para proteger a minha rede. Existe legislação para proteção de dados pessoais, em vigor. Temos de executar determinadas ações para garantir essa proteção. Não existe legislação que nos possamos regular. A competência das forças armadas em desenvolver ações militares no cyber espaço está protegida apenas por sermos forças armadas, uma legislação no âmbito militar. Pela constituição as forças armadas enquadradas para atuar em estado de guerra, defender o nosso território. Existem normativos, políticas, estratégias e orientações. Dificulta e torna exigente essa proteção de dados pessoais. Se detetamos que estamos a ser atacados, não podemos chegar lá, fazer hackback, contra-atacar com outro ataque. Se tivermos problemas com a sociedade civil temos de reencaminhar o problema para entidades competentes. O foco da cyber defesa será em situação de guerra. Portugal e outros países da união europeia em conjunto.

10 - Considera que Portugal esta a par com os restantes países da união europeia ou ainda existem atrasos?

Humano, em termos de qualidade e quantidade de recursos humanos, poucos recursos e conhecimentos humanos. Poucas pessoas para proteção das redes e poucos formadores para formar novos efetivos na proteção da cyber defesa. No mar, terra, ar e cyber espaço. Comparando com a aliança europeia o nosso país tem dimensão inferior aos nossos aliados. Já nem se fala em relação a dimensão dos Estados Unidos. O centro de cyber defesa está a fazer 3 anos de existência. Já se fala em reestruturar, unidade operacional ou unidade técnica com capacidade para o centro se deslocar a países de crise e eliminar a ameaça.

Entrevista realizada ao inspetor chefe da polícia judiciária Dr. Rogério Bravo da (UNC3T)

1 – Tendo em conta os recursos disponíveis, quais são as preocupações prioritárias da Polícia Judiciaria no combate ao cibercrime?

Malware, combate ao Malware, Fishing bancário e RANSOM WARE. Sabotagem implícita, quando cifra de dados eles ficam inutilizados. Abusos sexuais no cyber espaço. Preparação para pagamentos eletrónicos, “no cash”.

2 – Considera a o leque dos crimes elencados na lei do cibercrime que é condizente com os delitos praticados no ciberespaço?

Nossa doutrina no cyber espaço é cyber crime. Dentro do cyber crime só um é crime informático. Crimes contra indulto sexual, pedofilia, burlas ou honra são cyber crime, mas não crime informático. Ex. proteção de software não é crime informático. Só é crime informático quando nasce, cresce e morre dentro do cyber espaço, atacando a confidencialidade, integridade, disponibilidade e repúdio dos dados ou informação. Ex. Dano, sabotagem, dano de dados e falsidade informática.

3 – De que forma adquirem conhecimento dos crimes, através da monotorização ou de investigação?

Duas formas, ou as pessoas vítimas dos crimes se queixam, ou através de mecanismos de monitorização ou ainda através de mecanismos de comunicação de entidades externas nacionais ou internacionais.

4 A Polícia Judiciaria Tem meios técnicos e humanos adequados a realidade para o combate da cibercriminalidade?

Nunca temos todos os meios suficientes, queremos sempre mais e faremos por ter mais.

5 - O problema do cibercrime é hoje em dia Global, a Polícia Judiciaria considera a cooperação essencial entre as instituições tanto a nível interno com a nível externo?

A cooperação externa no que diz respeito à reação e cooperação a nível interno diz respeito a mitigação e troca de informação necessária.

6 - Como forma de fomentar essa cooperação, considera a realização de exercícios de treino proveitosos nesse sentido?

Grupos de trabalho e em conjunto com a INTERPOL já decorreram a algum tempo atrás. São proveitosos e fazem falta e deveriam ser incentivados.

7- A segurança é um bem de todos, considera que o público em geral tem consciência sobre o tema cibercrime?

Têm consciência sobre os outros, mas não consciência sobre si, acontece só aos outros e nunca em sua própria casa. O cyber crime precisa de ser trabalhado ao longo de todo o ano enão apenas no dia nacional da proteção e segurança.

8 - Como forma de reduzir a cibercriminalidade, a Polícia Judiciária desenvolve algum programa de formação e respetiva divulgação ao público?

Fazemos formação, mas não divulgação ao público. Formamos internamente inspetores e peritos. Formamos externamente no sentido preventivo com o cyber centro outras entidades públicas e privadas, conforme o público alvo. Programas de formação de norte a sul do país. Fazemos passar algumas mensagens a nível forense digital, com alguma discrição.

9 - Considera a Legislação atual suficiente e adequada para o desempenho das funções Polícia Judiciaria sobre o cibercrime?

Nunca é adequada porque as mudanças tecnológicas estão sempre à frente e a legislação não consegue acompanhar. Resta seguir princípios constitucionais.

10 - Considera que Portugal esta a par com os restantes países da união europeia ou ainda existem atrasos no combate ao cibercrime?

Os recursos humanos são escassos apenas. A nossa participação internacional é qualitativamente bem vista.

11 - O agente infiltrado digital é um meio oculto de investigação de último recuso ou de primeira linha?

Depende da gravidade dos casos. O agente infiltrado é utilizado nos casos mais graves e no cyber espaço isso acontece. Ser digital ou fora do mundo digital é o mesmo agente.

12 - Considera que o atual quadro jurídico-penal que regula o instituto do agente infiltrado no meio digital é apropriado ou carece de alguma alteração profunda?

De momento é suficiente. Pode acontecer de futuro, na parte da recolha de provas, que seja necessário existir aprimoramento para acompanhar as novas tecnologias.

BIBLIOGRAFIA

ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2011

AMADOR, Nelson, *Cibercrime em Portugal*, Trajetórias e Perspetivas de Futuro, Chiado Editora, Janeiro 2018, ISBN 978-989-52-1660-4

ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, A reforma do código de processo penal,* observações críticas sobre uma lei que podia e devia ter sido diferente, Coimbra Editora, 2009. ISBN 978-972-32-1726-1

ANDRADE, Manuel da Costa, *Sobre as proibições de Prova em processo Penal*, Coimbra: Coimbra Editora, 1992.

BRAZ, José, *Ciência, Tecnologia e Investigação Criminal,* Interdependência e Limites num Estado de Direito Democrático, Almedina, Setembo 2016, Reimpressão ISBN 978-972-40-5972-3

BRAZ, José, *Investigação Criminal,* a Organização, o Método e a Prova, os Desafios da Nova Criminalidade, 3ª ed, Almedina, Fevereiro 2017, ISBN 978-972-40-5317-2

BOLDT, Martin, *Privacy-Invasive Software, Blekinge Institute of Technology*, 2010

BUENO DE MATA, F., "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia", en PEREZ-CRUZ MARTÍN, A.J. y FERREIRO BAAMONDE, X. (Dirs.), Los retos del Poder Judicial ante la sociedad globalizada, Universidad de A Coruña, 2012

CAMPENHOUT, R.Q. Luc Van, *Manual de Investigação em ciências socias,* tradução Carvalho, Maria e Mendes, João,4ª ed, Gravida, Outubro 2005

CARMO, Hermano, FERREIRA, Manuela Malheiro – *Metologia da Investigação, Guia para Auto-aprendizagem,* Lisboa, Universidade Aberta, 1998, ISBN 972-674-231-4

CORREIA, Eduardo Perreira, coodenação, *Liberdade e segurança,* ISCPSI-ICPOL, Lisboa 2015, ISBN 978-972-8630-15-7

CORREIA, João Conde, *Prova digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público, Ano 35, n.º 139, julho-setembro 2014

DE LA ROSA CORTINA, J.M., "Los delitos de pornografía infantil. Aspectos penales, procesales y criminológicos, Tirant lo Blanch, Valencia, 2011

ERBSCHLEO, Michael, *Trojans, Worms and Spyware* – A Computer Security Professional's Guide to Malicious Code, Elsevier Butterworth–Heinemann, 2005

FARIA, José Miguel, *Criminologia,* Epanortologia Fundamento do Direito de Punir, ISCPSI-ICPOL, Lisboa 2014, ISBN 978-972-8630-11-9

FERNANDEZ TERUELO, J., *Cibercrime. Los delitos cometidos a través de internet, Constitutio Criminalis,* Carolina, Oviedo, 2007

FILIOL, Eric, *Computer viruses: from theory to application*, Springer, 2005

GONÇALVES, Albertino, *Métodos e Técnicas de investigação social I,* Instituto de ciências socias da Universidade do Minho, 2004

GONÇALVES, Fernando, ALVES, Manuel João, VALENTE, Manuel Monteiro Guedes, *Lei e Crime – O Agente Infiltrado vs o Agente Provocador, Os Princípios do Processo Penal*, Coimbra, Almedina, 2001.

JUDITH, Bell, *Como realizar um Projecto de Investigação,* 5ª ed, Gravida, 2010

KNIGHTLEY, Phillip, *Espiões e espionagem: História da segunda mais velha profissão do mundo,* tradução de MACHADO, Maria José Bellino, Círculo de Leitores, agosto 1990. ISN 972-420085-X

ONETO, Isabel, *O Agente infiltrado: Contributo para a compreensão do regime jurídico das acções encobertas,* Coimbra, Coimbra Editora, 2005. ISBN 972-32-1312-5

NEVES, Rita Castanheira, *As ingerências nas Comunicações Eletrónicas em Processo Penal,* Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova, 1ª ed., Coimbra editora, 2011

NICUESA, Luis Lafont, *El agente encuiberto en el proyecto de reforma de la ley de Enjuiciamento Criminala,* 2015

MATA MOUROS, Fátima, O agente infiltrado*, in revista do ministério publico, janeiro de 2001*

MARCONI, Marina de Andrade, LAKATOS, Eva Maria*, Fundamentos de Metodologia Científica,* 5ª ed, Editora Atlas, São Paulo 2003

MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal,* Coimbra, Almedina, 1999.

MESQUITA, Paulo dá, *Processo Penal, Prova e Sistema Judiciário,* 1ª ed., Coimbra Editora, setembro 2010, ISBN 978-972-32-1842-8

PEREIRA, Rui, "O "agente encoberto" na ordem jurídica portuguesa", *in Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa,* Vol. II, Coimbra Editora, 2005. ISBN 972-32-1344-3

RAMALHO, David Silva, *Métodos Ocultos de investigação Criminal em Ambiente Digital,* Edições Almedina, Maio 2017 ISBN 978-972-40-7000-1

RAMOS, Armando Dias, "*A prova digital em processo penal: o correio electrónico*", Chiado Editora, 1.º ed. Novembro 2014, ISBN 978-989-51- 2383-4

RODRIGUES, Benjamim Silva, "*Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital, Contributo para a Fundamentação da sua Autonomia*

Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital", Coimbra Editora, limitada, 2009. ISBN: 978-989-95779-5-4

RODRIGUES, Benjamim da Silva, *Da Prova Penal, Novos Métodos "Científicos" de Investigação Criminal nas Fronteiras das nossas Crenças,* Tomo IV, 1ed., Reis dos Livros, 2011

ROSSINI, Augusto, *Informática Telemática e Direito Penal,* Memória Jurídica Editora, São Paulo, 2004

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

SARMENTO, Manuela, Guia Prático sobre a metodologia científica, para elaboração, escrita e apresentação de teses de doutoramento, dissertações de mestrado e trabalhos de investigação aplicada, 3ª ed, Universidade Lusíada Editora, Lisboa

SILVA, Germano Marques da, *Bufos, Infiltrados, Provocadores e Arrependidos,* in Direito e Justiça*,* F.D.U. Católica, Vol. VIII, T. 2, 1994.

SILVA, Germano Marques da, *Meios Processuais Expeditos no Combate ao Crime Organizado (a Democracia em Perigo?)*. In Revista Lusíada n.º 3*,* 2005.

VALENTE, Manuel Monteiro Guedes, *A investigação do crime organizado in Criminalidade Organizada e Criminalidade de Massa,* (Coord. Manuel Monteiro Guedes Valente), Coimbra, Almedina, 2009.

VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 4ª Edição, Almedina, 2014. ISBN 978-972-40-5798-9

VENÂNCIO, Pedro Dias, "JusJornal" N.º 1182, 23 de Fevereiro de 2011, Editora Coimbra Editora, grupo WoltersKluwer

VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, 1.ª ed., Coimbra, Coimbra Editora, 2011 ISBN 978-972-32-1906-7

VERDELHO, Pedro, "*A obtenção de prova no ambiente digital"*, Revista do Ministério Público, Ano 25.º, nº 99 Julho-Setembro 2004

VICENTE, Dário Moura, *Problemática Internacional da Sociedade da Informação,* Edições Almedina, Setembro 2005

LEGISLAÇÃO

Constituição da República Portuguesa

Código Penal

Código Processo Penal

decreto-lei nº430/83, de 13 de dezembro (Regime jurídico do tráfico e consumo de estupefacientes)

decreto-lei n.º 15/93, de 22 janeiro

lei n.º 36/94, de 29 de setembro

lei 45/96, de 3 setembro

Lei 93/99

lei 101/2001, de 25 de agosto

lei 104/2001 lei da cooperação judiciária internacional em matéria penal

lei n.º 33/2010 para os meios técnicos de controlo a distância

Ley Orgânica nº 5/1999, de 13 de janeiro, Ley de Enjuiciamiento Criminal.

SITES NA INTERNET

https://www.infopedia.pt/dicionarios/lingua-portuguesa/espiar

https://fas.org/irp/doddir/dod/jp1_02.pdf

http://mbenedikt.com/royal_swedish_academy.pdf p4

https://pplware.sapo.pt/informacao/cerca-de-1000-pedofilos-localizados-gracas-a-crianca-virtual/

https://pplware.sapo.pt/informacao/sweetie-chumbada-como-prova-na-justica-portuguesa/

http://www.academia.edu/4691991/DOS_VEST%C3%8DGIOS_EM_AMBIENTE_DIGITAL_%C3%80_PROVA_DIGITAL_COMO_INTELLIGENCE