UNIVERSIDADE D
COIMBRA

Mara Leonora Antunes Ribeiro

O ESPAÇO DE ATUAÇÃO DO AGENTE ENCOBERTO DIGITAL: ENTRE A LEI DAS AÇÕES ENCOBERTAS E O ART. 19º DA LEI DO CIBERCRIME

Dissertação no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Criminais (conducente ao grau de Mestre) orientada pela Professora Doutora Susana Maria Aires de Sousa e apresentada à Faculdade de Direito da Universidade de Coimbra

Maio de 2022

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

DISSERTAÇÃO APRESENTADA À FACULDADE DE DIREITO DA UNIVERSIDADE DE COIMBRA NO ÂMBITO DO 2.º CICLO DE ESTUDOS EM CIÊNCIAS JURÍDICO-CRIMINAIS (CONDUCENTE AO GRAU DE MESTRE)

Mara Leonora Antunes Ribeiro

O ESPAÇO DE ATUAÇÃO DO AGENTE ENCOBERTO DIGITAL: ENTRE A LEI DAS AÇÕES ENCOBERTAS E O ART. 19º DA LEI DO CIBERCRIME

THE AREA OF ACTION OF THE DIGITAL UNDERWARD AGENT: BETWEEN THE LAW OF COVERED ACTIONS AND ART. 19TH OF THE CYBERCRIME LAW

DISSERTAÇÃO REALIZADA SOB A ORIENTAÇÃO DE:

Professora Doutora Susana Maria Aires de Sousa

Coimbra, 2022

“*Somos o resultado dos livros que lemos, das viagens que fazemos e das pessoas que amamos.”*
– Airton Ortiz.

Aos meus queridos pais.

AGRADECIMENTOS:

À minha orientadora, Professora Doutora Susana Aires de Sousa, pelos ensinamentos, conselhos e disponibilidade de sempre.

Aos meus pais, Arlindo e Iolanda, e irmão, Miguel, pilares estruturais da minha vida, sem os quais nada disto seria possível.

Ao meu companheiro de todas as horas, Jorge Edgar, por acreditar sempre em mim.

Aos meus amigos, em especial à Margarida, pela amizade que não esmorece com o passar dos anos.

RESUMO:

A delimitação do espaço jurídico da figura do agente encoberto digital constitui uma dúvida cujos contornos se tornam cada vez mais evidentes. A legislação processual que se dedica à regulação das suas atividades tem-se resumido à aplicação, por remissão ou por analogia, das regras processuais que foram pensadas para a investigação em ambiente físico.

Em face do exposto, a questão impõe-se continuamente: deverá esta figura e os problemas que convoca continuar a esgotar-se, por analogia, na realização do Regime Jurídico das Ações Encobertas, compensada unicamente pelo art. 19º da Lei do Cibercrime, não sendo, por consequência, reconhecida como um verdadeiro novo método de investigação criminal? Ou fará sentido conferir-lhe autonomia de regulamentação, concretizada através da criação de um novo Regime, desta vez idealizado e desenhado à luz da concreta atuação do agente encoberto digital e capaz de atender às suas caraterísticas especiais?

Assim, no presente estudo, o que se pretende analisar, depois de nos debruçarmos cuidadosamente sobre a Lei das Ações Encobertas e a Lei do Cibercrime, é como os dois Diplomas podem/devem ser articulados e se são bastantes para regular o *modus operandi* do agente encoberto digital. Não obstante os inúmeros problemas que a atuação da figura possa suscitar e que também procuraremos pontualmente invocar, o que pretendemos é analisar, com a humildade científica que nos cumpre, qual deverá ser efetivamente o seu espaço jurídico de atuação.

É em face dos desafios que as novas tecnologias suscitam ao nível da prevenção e prossecução criminal que esta será a questão que servirá de mote à presente dissertação, com o grande objetivo de dar o nosso contributo na procura do caminho regulamentador mais certeiro para este método oculto de investigação criminal.

PALAVRAS-CHAVE: métodos ocultos de investigação criminal; ações encobertas; agente encoberto digital; cibercrime; recolha de prova digital.

ABSTRACT:

The delimitation of the legal space of the figure of the digital undercover agent constitutes a doubt whose contours become increasingly evident. The procedural legislation dedicated to the regulation of its activities has been limited to the application, by reference or by analogy, of the procedural rules that were designed for research in a physical environment.

In view of the above, the question continually arises: should this figure and the problems it summons continue to be exhausted, by analogy, in the implementation of the Legal Regime for Covert Actions, compensated only by art. 19 of the Cybercrime Law, not being, therefore, recognized as a true new method of criminal investigation? Or does it make sense to grant it regulatory autonomy, implemented through the creation of a new Regime, this time idealized and designed in light of the concrete performance of the digital undercover agent capable of meeting its special characteristics?

Thus, in the present study, what we intend to analyze, after carefully looking into the Covert Actions Law and the Cybercrime Law, is how the two diplomas can/should be articulated and if they are enough to regulate the modus operandi of the agent digital covert. Notwithstanding the numerous problems that the role of the figure may raise and that we will also seek to invoke from time to time, what we intend is to analyze, with the scientific humility that fulfills us, what should effectively be its legal space of action.

It is in the face of the challenges that new technologies raise in terms of prevention and criminal prosecution that this will be the question that will serve as the theme of this dissertation, with the great objective of giving our contribution in the search for the most accurate regulatory path for this hidden method. of criminal investigation.

KEYWORDS: hidden methods of criminal investigation; covert actions; digital undercover agent; cybercrime; collection of digital evidence.

LISTA DE SIGLAS E ABREVIATURAS:

Al. – Alínea

Apud – Citado por

Art. – Artigo

Cfr. - Conforme

CP – Código Penal

CPP – Código Processo Penal

CRP – Constituição da República Portuguesa

DL – Decreto-Lei

GNR – Guarda Nacional Republicana

IP - Internet Protocol

JIC – Juiz de Instrução Criminal

LC – Lei do Cibercrime

LECrim - Ley de Enjuiciamiento Criminal

MP – Ministério Público

Nº - Número

Op. Cit. – Obra Citada

OPC – Órgão de Polícia Criminal

ONG – Organização Não Governamental

PIDE – Polícia Internacional e de Defesa do Estado

PJ – Polícia Judiciária

PSP – Polícia de Segurança Pública

RJAE – Regime Jurídico das Ações Encobertas

SEF – Serviços de Estrangeiros e Fronteiras

TEDH – Tribunal Europeu dos Direitos do Homem

STJ – Supremo Tribunal de Justiça

STS - Sentencia Tribunal Supremo

Ss – Seguintes

TC – Tribunal Constitucional

V.g. - Verbi gratia

ÍNDICE:

PARTE I: ENQUADRAMENTO CONCEPTUAL

1. Notas introdutórias: a Internet como «palco» da prática de crimes

O fenómeno da globalização e o aumento qualitativo e quantitativo da criminalidade trouxeram consigo novos desafios para o cerne do processo penal. Os tradicionais métodos de investigação criminal deixaram de ser capazes de dar uma resposta eficaz a uma criminalidade que se assume cada vez mais grave, violenta, organizada e transfronteiriça.

Este novo paradigma que se fez sentir, sobretudo, nas últimas duas décadas exigiu do Estado um reforço nas suas técnicas de investigação criminal que, embora perdendo transparência no seu *modus operandi,* com prejuízo para os direitos fundamentais dos cidadãos investigados, trouxe vantagens para a prevenção e prossecução criminais.

De facto, os riscos potenciados pela pós-modernidade redundaram numa consequência inevitável: o Estado abandona a velha máxima de que os direitos dos cidadãos devem ser encarados como *grilhões* que o limitam na sua atuação na luta contra a criminalidade, para passar a ser o responsável pela punição dos culpados e pela proteção dos inocentes, ainda que para tanto seja necessária a frustração, em certa medida, de direitos fundamentais do cidadão investigado.[1] É nesse contexto que os métodos ocultos de investigação criminal ganham protagonismo e, com eles, a figura do agente encoberto, que merecerá destaque na presente dissertação.

Hoje atrevemo-nos a afirmar que, de entre todos os métodos de investigação criminal que estão consagrados no nosso ordenamento jurídico, investigar o agente encoberto será dos mais difíceis. Enquanto forma de atuação pertencente à categoria dos métodos ocultos de investigação, a ação encoberta concretiza uma "intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam"[2], provocando uma considerável danosidade nos seus direitos fundamentais. Assim se compreende que estas

[1] DAVID SILVA RAMALHO, *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra: Edições Almedina, 2019. Pg. 203.
[2] MANUEL DA COSTA ANDRADE, *Bruscamente no verão passado: a reforma do Código de Processo Penal: observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora, 2009. Pg. 104.

ações vivam envoltas numa rede de paradoxos e conflitos doutrinais propícios ao comentário crítico.

Para que melhor as possamos compreender, historicamente, as ações encobertas, método de investigação oculto por excelência, podem ser reconduzidas ao surgimento na França, no século XVII, do chamado "*agente provocateur*". Este agente provocador, criado no contexto do regime absolutista francês, com vista a combater a elevada criminalidade que à época se fazia sentir, mas também, e essencialmente, a desenvolver atividades de espionagem política numa tentativa de eventual eliminação dos inimigos políticos do regime, só veio a encontrar um enquadramento jurídico-dogmático na Alemanha, em meados de 1858, com os estudos de *Glaser,* sobre o dolo do instigador, ponto de partida da construção jurídica da figura.[3]

No nosso ordenamento jurídico, a figura do agente encoberto remonta às Ordenações Filipinas, ao ano de 1603, onde começou a evidenciar-se o recurso aos informadores políticos e delatores de crime.[4] A regulamentação das ações encobertas, embora tardia, veio a materializar-se no DL nº 430/83, de 13 de dezembro, em que se regulou pela primeira vez a questão da responsabilidade criminal do funcionário de investigação criminal. A esse Diploma seguiram-se outros - mormente o DL Nº 15/93 de 22 janeiro, a Lei nº 36/94 de 29 de setembro, a Lei nº45/96 de 3 de setembro e a Lei nº 101/2001 de 25 de agosto - que vieram alargar o campo de atuação do agente encoberto, deixando de estar apenas vedado às investigações relacionadas com o tráfico de droga e com a criminalidade económico-financeira, para também se situar ao nível da prevenção e investigação criminais de outro tipo de criminalidade grave e violenta.[5]

A ampliação do âmbito de incidência das ações encobertas poderá encontrar justificação na insuficiência dos meios investigatórios tradicionais perante a especial gravidade e sofisticação do modo de execução com que se cada vez mais se apresentam os crimes da atualidade.[6] De facto, perante a proliferação de crimes praticados com recurso às novas tecnologias, os Estados cada vez mais necessitam de se munir de novos modos de

[3] SUSANA AIRES DE SOUSA, *Agent Provocateur e meios enganosos de prova. Algumas reflexões, in* Separata de Liber Discipulorum para Jorge de Figueiredo Dias." Coimbra: Coimbra Editora, 2003. Pg. 1223 e 1224.
[4] ARMANDO DIAS RAMOS, *O agente encoberto digital: meios especiais e técnicos de investigação criminal,* Coimbra: Edições Almedina, 2022. Pg. 32.
[5] Como o terrorismo, a corrupção e o branqueamento de capitais.
[6] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.*, Pg. 204.

investigação, de adaptar e reforçar a prevenção e repressão criminais e atualizar as suas legislações processuais. A utilização dos antigos e convencionais métodos de investigação já não é mais capaz, por si só, de desmembrar os grandes grupos criminosos que se movem através de métodos cada vez mais inovadores.[7]

Como evidencia Armando Dias Ramos, a Internet e, com ela, o correio eletrónico, as comunicações por VoIP e as mensagens instantâneas, mudaram radicalmente a vida do Homem. A comunicação entre as pessoas é hoje praticamente instantânea e gratuita e pode ser feita mesmo a milhares de quilómetros de distância.[8] Porém, se é verdade que este desenvolvimento tecnológico trouxe facilidades para a vida em sociedade, também se refletiu no mundo da criminalidade, que das suas potencialidades aproveitou: dele resultaram novas formas e meios de praticar crimes e o aumento do número de vítimas que todos os dias são alvo de distintas formas de ataque, através de todo o tipo de dispositivos (*smartphones, tablets, notebooks*, entre outros). Hoje estão, assim, criadas todas as condições necessárias para garantir o sucesso dos crimes informático-digitais.[9]

No que aos cibercrimes respeita cumpre referir que as vantagens que beneficiam não são equiparáveis às que se fazem sentir entre os crimes praticados em ambiente físico: a investigação não se encontra delimitada pelas fronteiras físicas, o local da prática do crime não é facilmente percecionável, os crimes são levados a cabo com recurso a técnicas de anonimização[10] que tornam difícil a identificação do seu autor e a cooperação internacional judiciária na sua investigação releva-se ainda algo deficitária.[11] Por outro lado, as

---

[7] FREDERICO PELLUCCI, *A atuação dos Agentes Encobertos e Infiltrados nos Canais Abertos e Fechados de Comunicação em Ambiente Informático-Digital in* Novos Desafios da Prova Penal, Coordenação Paulo de Sousa Mendes e Rui Soares Pereira, Almedina, 2020. Pg. 236.

[8] DUARTE RODRIGUES NUNES, Duarte Rodrigues, *O agente infiltrado online no direito português in* Revista Ultracontinental de Literatura Jurídica, Ed. Associação de Letras Jurídicas de Montes Claros, Montes Claros, v. 2, n. 3, set.-dez. 2021. Pg. 34.

[9] Também designados por cibercrimes, podem ser definidos como "aqueles tipos de crime cujos sistemas informáticos podem servir de instrumento para a perpetração de crimes, ou cujos instrumentos informáticos são alvo desses mesmos ataques, pelo que o ilícito praticado através de equipamentos informáticos não se assemelhará aos tradicionalmente previstos pelo legislador penalista". *Cfr.* JOSÉ PEDRO FREITAS, *Os meios de obtenção de prova digital na investigação criminal. O regime jurídico dos serviços de correio eletrónico e de mensagens curtas*, Braga: Nova Causa Edições Jurídicas, 2020. Pg. 56.

[10] Note-se que tais técnicas se revelam particularmente perigosas atendendo ao facto de serem facilmente utilizadas por qualquer pessoa. Na verdade, como bem nota Armando Dias Ramos, qualquer pessoa pode facilmente tornar-se apta a praticar crimes em ambiente informático-digital, havendo inclusivamente na Internet muitas páginas explicativas, fóruns de debate e de treinamento e vídeos no Youtube, por exemplo, de como ocultar a identificação do IP do utilizador. *Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.,* Pg. 118 (Nota de pé de página nº 252).

[11] *Ibidem.* Pg. 118.

organizações cibercriminosas funcionam hoje como verdadeiras "empresas", contando com agentes especializados para levar a cabo todo o tipo de ataques, extorsões e fraudes, como programadores, distribuidores, técnicos especializados, *hackers*, defraudadores, vendedores de *hosting*, branqueadores e líderes da organização.[12] Existindo, assim, diferentes níveis de especialização entre os delinquentes em matéria de crimes informáticos, tornam-se extremamente fáceis operações que seriam aparentemente difíceis como a obtenção de credenciais de acesso (ao *homebanking*, a cartões de débito ou crédito, ao email, a redes sociais ou a *sites* de natureza reservada que requerem a introdução de uma *password*) e a cópia ou acesso a dados armazenados em sistemas informáticos alheios.[13]

Para além disso, cumpre apontar que a prática de crimes por detrás de um dispositivo se releva também efetivamente mais segura para os criminosos,[14] apresentando, nas palavras de Armando Dias Ramos, uma "tríplice vantagem": a desterritorialização da prática criminosa, a rapidez da atuação e a eficácia das ações criminosas sob o manto do anonimato.[15] De facto, a rapidez, a volatilidade e o anonimato proporcionado pelo uso de redes criptografas, VPN's ou programas específicos de cifragem de conteúdos e comunicações informáticas permitem uma execução criminosa perfeita e a eliminação de eventuais provas incriminadoras[16], transformando a criminalidade informático-digital verdadeiramente "paradisíaca"[17]. Note-se que desta tríplice vantagem beneficiaram já casos paradigmáticos como o do *Silk Road,* nos Estados Unidos da América, em que durante mais de 2 anos, o *website The Silk Road,* um mercado digital *online,* criado na *Darkweb,* destinado à venda de produtos e serviços ilegais (essencialmente, estupefacientes e armas) em moeda *bitcoin,* foi palco da prática de inúmeros crimes e se manteve incólume à ação da justiça norte-americana.[18]

---

[12] PANDA SECURITY, *El mercado negro del Cibercrimen al descubierto*. Disponível em: https://www.pandasecurity.com/es/mediacenter/src/uploads/2014/07/Mercado-Negro-del-Cybercrimen.pdf [Acesso em: 11 de nov. de 2021). Pg. 9.
[13] DUARTE RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 37 e 38.
[14] MARCELO TEMPERINI, MAXIMILIANO MACEDO, *Nuevas Herramientas de Investigación penal: el agente encubierto digital in* "*Cibercrimen: aspectos de derecho penal y procesal penal: cooperación internacional: recolección de evidencia digital: responsabilidad de los proveedores de servicios de internet*", Montevideo Buenos Aires, 2016. Pg. 481.
[15] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 12.
[16] DUARTE RODRIGUES NUNES, *O agente infiltrado … Op. Cit.* Pg. 37.
[17] ARMANDO DIAS RAMOS, *O agente encoberto digital…op. Cit.* Pg. 80.
[18] *Ibidem*. Pg. 230 a 234.

E é em face do exposto que, cada vez mais, uma parte significativa da doutrina tem vindo a defender a utilidade e excelência dos métodos ocultos de investigação na resposta a este tipo de criminalidade particularmente difícil. Neste sentido se manifesta Duarte Rodrigues Nunes, ao defender que a investigação através de métodos ocultos se revela fulcral, sobretudo, quando em causa estão factos ilícitos praticados na *Deep Web*[19], em que existem sérias dificuldades em nela aceder, bem como em identificar e localizar os autores do crime e respetivas vítimas. Nesses casos, só a atuação do agente encoberto digital, com a sua integração na comunidade o*nline* e interação com os suspeitos da prática de crimes permite neutralizar os obstáculos da cibercriminalidade.[20] Pense-se, a título de exemplo, no combate à disseminação da pornografia infantil ou da pedofilia *online,* em que as ações encobertas digitais poderão constituir mesmo a única técnica especial de investigação capaz de ultrapassar de forma eficiente a ausência de limites espaciais e temporais do submundo virtual.[21]

Sucede que, não obstante estes métodos de investigação se reputarem essenciais para fazer prova de determinados factos ilícitos, não deixam de constituir "técnica[s] de investigação de moral duvidosa"[22], na medida em que acabam por atentar às exigências de um Estado de Direito Democrático ao restringir de forma particularmente intensa os direitos,

---

[19] A *Deep Web,* também chamada de *Deepnet* ou *Undernet (*"internet profunda") corresponde a uma parte da *Web* que não é acessível pelos mecanismos de busca comuns, como o *Google*, sendo assim oculta ao grande público. Recorrendo analogicamente à imagem de um *iceberg,* a *Deep Web* corresponderá à parte imersa que, se por um lado não é acessível à maioria dos navegadores, por outro, respeita à maior parte da Internet, em contraste com a *Surface Web,* a parte exposta que é composta pela Internet tal como a conhecemos. Segundo Armando Dias Ramos, dentro da *Deep Web* podemos ainda encontrar a *Opaca Web ou Dark Weeb, a Web Privada, a Web Proprietária e a Web realmente invisível,* subdivisões onde se encontrarão a maioria dos conteúdos ilícitos e cujo material intencionalmente oculto é inacessível através de navegadores *Web* padrão. (*cfr.* ARMANDO DIAS RAMOS, *A prova digital em processo penal: o correio eletrónico*, 2ª Edição atualizada e ampliada, Lisboa: Chiado Editora, 2014. Pg. 144 e 145). Importa ainda referir que o facto de os conteúdos patentes na *Darkweb* não estarem indexados exige que se recorra a *softwares* específicos, como o *Freenet* (rede anónima de computadores que funcionam com armazenamento compartilhado e distribuído), o *I2P (*rede anónima, com uma única camada de rede, na qual os aplicativos de computadores, entre eles, podem usar cominicações criptografadas de ponta-a-ponta) e o *GNUnet* (aplicação para partilha de ficheiros *peer-to-peer* [P2P] de forma descentralizada e anónima). (*Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.,* Pg. 147 e 148).

[20] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada,* 1ª Edição, Coimbra: Gestlegal, 2019. Pg. 841.

[21] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 238.

[22] MANUEL MONTEIRO GUEDES VALENTE, *Teoria Geral do Direito Policial,* 2.ª Edição, Coimbra: Almedina, 2009. Pg. 406. Também neste sentido: FERNANDO GONÇALVES, JOÃO MANUEL ALVES, *Crime. Medidas de Coação e Prova. O agente infiltrado, encoberto e provocador*, Coimbra: Edições Almedina, 2015. Pg. 300

liberdades e garantias dos cidadãos investigados, em particular a sua dignidade humana (art. 1º da CRP), a sua integridade moral (art. 25º CRP) e, sobretudo, a intimidade da sua vida privada (art. 26º CRP) – todos eles constitucionalmente reconhecidos. Assim, direitos como a privacidade, autodeterminação informacional, confidencialidade, inviolabilidade do domicílio, liberdade de expressão e, em caso de recurso a ações encobertas digitais, a integridade e confidencialidade dos sistemas técnico-informacionais[23], são invariavelmente colocados em cheque.[24]

Note-se ainda que se já eram muitos os problemas e as dúvidas que se levantavam em torno da admissibilidade dos clássicos meios de prova, agora a prova digital[25] e, em particular, a prova digital obtida por meio de uma ação encoberta, torna-se ainda mais controversa. Não podemos olvidar que as razões que tornam as ações encobertas um método de excelência no combate à criminalidade organizada são também as mesmas circunstâncias que as tornam dúbias: efetivamente, este método de investigação tem como caraterística essencial a quebra da *affetio soccietatis,* princípio estrutural na criminalidade organizada na resistência à Justiça, na medida em que encoraja a exploração da infidelidade criminosa e a introdução de brechas nas organizações criminosas. Assim, através deste tipo de método de investigação, o Estado rompe a *omertá* – o silêncio mafioso -, penetrando no interior das organizações criminosas com o objetivo de produzir prova processual, ao mesmo tempo que as divide e enfraquece.[26] Nas palavras de Frederico Pellucii, "a pedra angular desse meio de investigação reside, portanto, na existência d[e] [um] engano"[27], sendo essa circunstância que o torna questionável.

---

[23] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade… Op. Cit*. Pg. 830; MANUEL DA COSTA ANDRADE, *Bruscamente no verão passado… Op. Cit.* Pg. 106 e 107.

[24] Também neste sentido: JOSÉ CARLOS VIEIRA DE ANDRADE, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 6ª Edição, Coimbra: Almedina, 2019. Pg. 62.

[25] Entendida como a "prova produzida a partir de dados em formato digital (na forma binária), que «são manipulados, armazenados ou comunicados através de qualquer dispositivo, computador ou sistema informático, ou transmitidos através de um sistema de comunicação» (…) Através da recolha de prova em ambiente digital conseguirá aceder-se a dados informáticos tão variados como ficheiros de imagem ou de vídeo, conteúdo de *e-mails*, diários eletrónicos, dados de tráfego, dados de localização, entre outros.". *Cfr.* SÓNIA FIGALDO, *A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo in* A inteligência Artificial no Direito Penal [Coord: Anabela Miranda Rodrigues], Coimbra: Edições Almedina, 2020. Pg. 133.

[26] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 240.

[27] *Ibidem.* Pg. 244

Ora, embora o processo penal tenha como finalidades primordiais a descoberta da verdade material (aqui pugnada no sentido de uma "verdade processualmente válida"[28]) e, com ela, a realização da justiça no caso concreto, não poderá perder de vista o respeito pelos limites da dignidade humana e dos princípios do Estado de Direito democrático em matéria de obtenção de prova. Daí que aquelas primeiras finalidades sejam hoje temperadas, essencialmente, pelo art. 126º do CPP que trouxe consigo, por um lado, proibições de prova absolutas (densificadas nos seus nºs 1 e 2) – mormente aquelas que tenham como alvo "direitos fundamentais cuja compressão é absolutamente intolerável em processo penal, não só por inultrapassável corrosão da pretendida s*uperioridade ética do Estado,* mas acima de tudo porquanto intrinsecamente afectos ao núcleo da personalidade"[29], como o direito à integridade pessoal – e, por outro, proibições de prova relativas (introduzidas por via do seu nº 3) – sempre que em causa esteja a produção de prova que, embora possa ser valorada, fora alcançada em moldes manifestamente abusivos, isto é, em violação do princípio da proporcionalidade, como sucede tipicamente com os casos de intromissão na vida privada, domicílio, correspondência ou telecomunicações.[30]

É certo ainda que se a admissibilidade da prova obtida através de um método oculto de investigação criminal, mesmo com respeito pelos parâmetros legalmente exigidos, carecia já de uma ponderação casuística capaz de avaliar a sua necessidade e adequação em função da gravidade do crime e do circunstancialismo concreto, a admissibilidade da prova digital deverá ser ladeada de maiores cautelas, atendendo, desde logo, à sua concreta natureza. De facto, como refere David Silva Ramalho, o acesso a sistemas informáticos – forma mais comum de atuação do agente encoberto digital - torna-se cada vez mais fácil e a realização de atividades de natureza sensível (como operações bancárias, o exercício de funções afetas a profissões sujeitas a segredo profissional, o armazenamento de dados e documentos pessoais em formato digital bem assim como de correspondência, vídeos e fotografias pessoais) estende-se ao cidadão comum sem ser necessários profundos conhecimentos informáticos. Esta banalização torna a prova digital particularmente perigosa, de tal modo

[28] PAULO DÁ MESQUITA, *A Prova do Crime e o que se disse Antes do Julgamento – Estudo sobre a Prova no Processo Penal Português, à Luz do Sistema Norte-Americano,* Coimbra: Coimbra Editora, 2011. Pg. 266.
[29] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 187
[30] *Ibidem;* Assim, estas proibições de prova relativas admitem, em casos circunstanciados, dentro do exigido pelo princípio da proporcionalidade e em respeito pela administração da justiça penal, a compressão de certos direitos com consagração constitucional. *Cfr.* MANUEL DA COSTA ANDRADE, *Bruscamente no verão passado… Op. Cit.* Pg. 136 e 137;

que "a mera pesquisa ou apreensão de dados informáticos em largos acervos de informação, ainda que formalmente cumpridora dos requisitos legais, deva ser sujeita a um especial cuidado na ponderação da admissibilidade da sua valoração"[31].

2. As ações encobertas

2.1. Os atores: da infiltração à provocação

A compreensão das ações encobertas e tudo o que elas pressupõem reclama a desmitificação do seu conceito. Inicialmente as figuras do "agente encoberto", do "agente infiltrado" e do "agente provocador" eram reconduzidas ao conceito amplo de "homens de confiança" -, isto é, às "testemunhas que colabora[vam] com as instâncias formais de perseguição penal, tendo como contrapartida a promessa de confidencialidade da sua identidade e actividade"[32] - não sendo, portanto, feita qualquer distinção entre elas.

No entanto, a dada altura, em face das diferentes facetas que os homens de confiança foram assumindo, começou a sentir-se a necessidade de se restringir os conceitos. Atualmente, o conceito de "homem de confiança" assume contornos diferentes, dizendo agora respeito a uma pessoa não pertencente às forças policiais e cuja conduta poderá configurar a atuação de um agente encoberto, infiltrado ou provocador, conforme o circunstancialismo concreto. Assim, nas palavras de Duarte Rodrigues Nunes, hoje a conduta do «homem de confiança» "corresponderá à atuação do tipo de agente que «encarnar»".[33]

Deste modo, alguma parte da doutrina começou por propor um critério distintivo baseado no grau de ingerência das referidas figuras nos ilícitos criminosos e na forma como essa ingerência perturbaria os direitos e liberdades fundamentais dos cidadãos investigados. Alves Meireis, inserindo-se nessa corrente doutrinal, identifica o agente infiltrado ao "agente de autoridade ou cidadão particular que actu[a] de forma concertada com a polícia, e que, sem relevar a sua identidade ou qualidade e com o fim de obter provas para a incriminação do suspeito, ou então, simplesmente para a obtenção da notícia do crime, ganha a sua

[31] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 202.
[32] MANUEL DA COSTA ANDRADE, *Sobre as Proibições de Prova em Processo Penal* (Reimpressão), Coimbra: Coimbra Editora, 2013. Pg. 220.
[33] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade… Op. Cit.* Pg. 835.

confiança pessoal, mantendo-se a par dos acontecimentos, acompanhando a execução dos factos, praticando actos de execução se necessário for, de forma a conseguir a informação necessária ao fim a que se propõe."[34]; e o agente encoberto a um "polícia à paisana", isto é, a um "agente da autoridade, ou alguém que com ele actua de forma concertada, que, sem revelar a sua identidade ou qualidade, frequenta os meios conotados com o crime na esperança de descobrir possíveis indícios de matéria criminal."[35]

Assim, partindo daquelas premissas, o que distinguiria o agente encoberto do infiltrado seria o facto de a presença e a qualidade daquele primeiro não determinar nem influenciar de forma alguma o rumo dos acontecimentos, na medida em que naquele lugar e naquele momento poderia estar qualquer outra pessoa e tudo aconteceria da mesma forma. Por conseguinte, enquanto os agentes encobertos se limitariam a observar e a recolher o material probatório, não contribuindo para a prática do crime nem restringindo, de forma alguma, os direitos fundamentais do autor do ilícito investigado (sendo, portanto, a prática criminosa o fruto da iniciativa livre do criminoso), o agente infiltrado, para além de observar todo o meio criminoso envolvente, procuraria envolver-se nele e conquistar a confiança do autor da prática do crime, de modo a tornar-se parte integrante da organização criminosa e através dela obter algumas informações, declarações e outras confidências acerca do delito.[36]

Contra aquela destrinça conceptual se manifesta David Silva Ramalho, de acordo com o qual a distinção entre as figuras acaba por se revelar "inútil"[37], na medida em que, como explica, "ou o conceito (…) se refere a órgãos de polícia criminal que não têm de usar farda no exercício da sua função, caso em que poderão ser sempre considerados agentes encobertos nesta acepção, ou se refere a órgãos de polícia criminal tipicamente sujeitos à

---

[34] MANUEL AUGUSTO ALVES MEIREIS, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal*, Coimbra: Almedina, 1999. Pg. 163 e 164

[35] *Ibidem.* Pg. 192; Também pugnando pela antonímia entre as palavras: FERNANDO GONÇALVES; MANUEL MONTEIRO GUEDES VALENTE; JOÃO MANUEL ALVES, *O novo regime jurídico do agente infiltrado: Comentado e Anotado - Legislação Complementar.* Coimbra: Editora Almedina, 2001. Pg. 40 e 41.

[36] Também neste sentido dispõe Duarte Nunes, identificando ainda como outro critério de distinção entre as figuras a duração da atuação do agente, partindo do pressuposto que a atuação do agente infiltrado será mais prolongada. (Cf. DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade…Op. Cit.* Pg. 836). Contrariamente, Isabel Oneto entende ser o agente encoberto uma subespécie do agente infiltrado, não havendo uma autonomia conceptual. Para a Autora o agente encoberto corresponderá, por definição, àquilo que Meireis identifica como "polícia à paisana", tratando-se daquele que "oculta a sua qualidade ou identidade no seu relacionamento com terceiros, mantendo-os na sua ignorância para ganhar a sua confiança*". Cfr.* ISABEL ONETO, *O Agente Infiltrado: Contributo para a compreensão do regime jurídico das ações encobertas.* Coimbra: Coimbra Editora, 2005. Pg. 139.

[37] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 289.

utilização de farda que, durante o serviço, frequentam locais onde suspeitam que podem ocorrer ilícitos criminais, ocultando a sua identidade ou qualidade, caso em que se trata materialmente de uma acção encoberta subsumível ao regime da Lei nº 101/2001"[38]. No seu entender, a distinção não só é inútil como também "gera confusão"[39], porquanto considera que admiti-la seria concluir pela atipicidade deste meio de obtenção de prova e pelo seu enquadramento no art. 125º do CPP, com o inconveniente da exclusão do conceito de agente encoberto do regime legal das ações encobertas e a consequente atribuição da designação de *infiltrado* (inexistente na lei) ao agente encoberto (figura consagrada na lei).[40]

Ora, entre nós, à semelhança do que defende o autor *supra* citado, uma tal distinção, quando pensada no contexto do espaço físico, não traria qualquer utilidade material, porque obrigaria a que se alterasse toda a legislação, com a substituição do adjetivo "encoberto" (a única que a lei conhece) pelo de "infiltrado" (figura que não existe na lei). Assim, mesmo na hipótese de serem encontradas algumas diferenças pontuais entre as figuras do agente encoberto e infiltrado, subscrevemos inteiramente o pensamento de Sandra Pereira, de acordo com a qual a distinção não é de suma importância, na medida em que a Lei nº 101/2001 sempre será aplicável a ambas as figuras, independentemente de serem autonomizáveis ou não.[41]

Por outro lado, concordamos com Armando Dias Ramos, na parte em que o autor, embora aceitando as duas expressões como sinónimas, admite inclinar-se para a expressão "encoberto" porque, para além de ser assim que o RJAE a ela se refere, a expressão "infiltrado" tem uma conotação ligada aos tempos ditatoriais, sendo-lhe associada a espionagem sem escrúpulos e a delação com o intuito de receber recompensas.[42]

Expostos estes termos, cumpre referir que se em ambiente físico a distinção anterior não assume relevância, nem é conveniente, em espaço digital poderá voltar a ganhar força.

---

[38] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 289 e 290*;* Também Isabel Oneto se manifesta neste sentido, entendendo que, independentemente de as figuras serem ou não autonomizáveis, a verdade é que a Lei nº 101/2001 sempre lhes será aplicável. *Cfr.* ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 139.
[39] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 289.
[40] *Ibidem.* Pg. 290.
[41] SANDRA PEREIRA, *A recolha de prova por agente infiltrado*, *in* Prova Criminal e Direito de Defesa: Estudos sobre teoria da prova e garantias de defesa em processo penal. Ana Rita Fidalgo.. [et al.] / coordenação [de] Teresa Pizarro Beleza, Frederico de Lacerda da Costa Pinto. Coimbra: Editora Almedina, 2010. Pg. 143.
[42] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 56.

De facto, neste específico contexto, os conceitos assumem novos contornos e as particularidades do mundo virtual poderão reclamar a separação entre as figuras.[43]

Neste sentido, alguns autores, pugnando pela distinção entre agente encoberto e agente infiltrado digitais, associam a conduta do primeiro à simples criação de uma página de Internet com o intuito de identificar suspeitos da prática de um determinado crime (*v.g.* em matéria de pornografia infantil), sem para isso seja necessária a utilização de dados identificativos fictícios[44], casos em que inexiste, portanto, qualquer intervenção do agente no ilícito criminoso ou qualquer contacto com os seus intervenientes. Duarte Rodrigues Nunes, inserindo-se nessa posição doutrinária, considera que continuará a estar em causa a figura do agente encoberto digital sempre que se limite a participar em *chats, websites*, *blogs* ou fóruns livremente acessíveis (ainda que mediante um registo prévio e a utilização de um *nickname*) e a observar o seu conteúdo, de tal forma que o seu *modus operandi* não se distingue dos demais frequentadores. [45] Já o agente infiltrado digital, diferentemente, para além de patrulhar "os sítios da Internet, *chats ou newsgroups* abertos ou acedidos com o consentimento de um dos participantes, de redes P2P [*peer to peer*] e outras «zonas de risco» do Mundo virtual"[46], procura também por se introduzir, de forma mais ativa nele, movendo-se através de uma identidade fictícia que lhe permita conquistar a confiança dos investigados e, com ela, o acompanhamento de todos os atos que integram o *iter crimini,* sem, no entanto, determinar os suspeitos à prática do crime.[47]

Deste modo, a destrinça anteriormente proposta parte daquele mesmo critério do grau de ingerência do agente no ilícito, que vimos ser utilizado quanto às investigações que decorrem em ambiente físico. Tal como sucede com o agente encoberto físico, a que vimos ser-lhe doutrinalmente associada uma conduta mais passiva, também a atividade do agente encoberto digital traduzir-se-ia na mera observação atenta de canais «abertos» de comunicação, isto é, sítios da internet de acesso livre e público (eventualmente relacionados

[43] Neste sentido prossegue FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 260 e 261.
[44] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade…" Op. Cit.* Pg. 832.
[45] *Idem, O agente infiltrado… Op. Cit.* Pg. 55.
[46] *Ibidem.*
[47] Tal destrinça poderá ancorar-se na lógica que está subjacente à distinção que é feita por outra corrente doutrinal, a partir do artigo 10º, parágrafo 3º da Lei de Organizações Criminosas (Lei 12.850/13), entre *light cover* e *deep cover:* a *light cover* ou, também designada, infiltração leve, consiste num método oculto de investigação em que o respetivo agente não se envolve no meio criminoso por mais de seis meses; já a *deep cover* ou infiltração profunda diz respeito aos casos em que o agente infiltrado mergulha totalmente no âmbito da organização criminosa, sob uma identidade fictícia e praticamente não mantém contacto com o exterior por um período superior a seis meses; Sobre estas modalidades de operações encobertas veja-se ainda, mais desenvolvidamente: ISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 81 a 84.

com práticas criminosas), através da criação e utilização de um *nickname* ou *username*. Assim, a sua atividade corresponderia àquilo a que se chama comummente de "ciberpatrulha", não se verificando qualquer outra interação mais expressiva entre o agente e os sujeitos investigados. Já o agente infiltrado, no plano informático-digital, diferentemente, frequentando canais de comunicação não só «abertos», mas essencialmente «fechados», socorrer-se-ia de uma verdadeira identidade fictícia para, dessa forma, conquistar a confiança dos investigados, manter-se a par dos acontecimentos e acompanhar a execução dos factos criminosos. Assim, o agente infiltrado procuraria, portanto, por interagir mais ativamente com os outros participantes nas diversas plataformas de comunicação (sobretudo de acesso reservado), não se limitando a observa-las, de tal forma que a prática de atos ilícitos preparatórios ou de execução, na eventualidade de serem necessários, estaria dentro do espetro do seu modo de atuação, sem, no entanto, determinar os investigados à prática criminosa.[48]

Entre nós, independentemente da posição que se adote quanto à distinção entre agente encoberto digital e agente infiltrado digital, cremos que, na verdade, o cerne do problema não reside na designação que lhe seja atribuída. A problemática centra-se antes no espaço em que o agente (encoberto e/ou infiltrado) atua. Será o facto de as investigações decorrerem num canal «aberto» ou num canal «fechado» de comunicação que acabará por determinar especificidades diferentes ao nível do grau de penetração do agente no cerne criminoso e na necessidade de as suas atividades estarem ou não dependentes da obtenção de uma prévia autorização judicial. Assim, como teremos oportunidade de explanar em momento ulterior mais oportuno, será, nas palavras de Pellucci, "o modo de atuação do agente que determinará a necessidade ou não de se utilizar o regramento legal"[49], com a imposição de limites à sua atuação e a sua sujeição ao RAJE.

Finalmente, uma última figura de relevo nestas matérias, o agente provocador corresponde àquele que procura incitar e levar o sujeito investigado à prática do crime, não se limitando a observar e a desenvolver contactos capazes de gerar a confiança dos investigados, como sucede tipicamente com as duas figuras anteriores. Posto isto, no plano físico, o agente provocador corresponde àquele que, socorrendo-se de uma identidade

[48] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 262
[49] *Ibidem*. Pg. 261.

fictícia física, "convence outrem a cometer um crime que, não fosse a atuação do agente provocador, jamais cometeria"[50] e, no plano informático-digital, àquele que, semelhantemente, também o faz recorrendo a uma identidade fictícia virtual, através da utilização de um *username* ou *nickname.*

Nesta figura de agente provocador agora em análise poderá figurar tanto um agente de autoridade que instiga o suspeito à prática do crime com o intuito de progredir na carreira ou simplesmente combater o crime, como um particular que atua com um desejo de vingança ou de concretização de um plano idealizado para obter benefícios com a condenação do provocado.[51] Nestes casos, sendo a prova produzida o resultado da violação de importantes garantias processuais do provocado, acaba por resvalar para o domínio dos métodos proibidos de prova (nos exatos termos do art. 126º/2/a) CPP).[52]

Sucede que também a figura do agente provocador não reúne consenso, sobretudo quando pensada no prisma da intenção por ele prosseguida: alguns autores, como Fernando Gonçalves, Manuel Alves, João Valente e Manuel Monteiro Guedes, apontam ao agente provocador um verdadeiro dolo de consumação, na medida em que entendem que ele *"cria o próprio crime, porque induz o suspeito à prática de atos ilícitos, instigando-o e alimentando o crime..."*[53]*;* Já outros autores, contrariamente, desconsideram a possibilidade de ser reconhecido ao agente um verdadeiro dolo na consumação do crime. Neste sentido se manifesta Cristina Maglie que considera que o «*agent provocateur*» não tem como objetivo imediato a consumação do crime. No seu entendimento, o desenvolvimento de uma conduta criminosa pelo agente representa apenas o instrumento por meio do qual ele poderá atingir o objetivo real por ele perseguido que é exatamente que o provocado seja processado e responsabilizado criminalmente. [54] Em virtude disso, prossegue a autora afirmando que "o

---

[50] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade… Op. Cit.* Pg. 833.
[51] MANUEL AUGUSTO ALVES MEIREIS, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal*, Coimbra: Almedina, 1999. Pg. 156.
[52] MANUEL COSTA ANDRADE, *Sobre as proibições… Op. Cit.* Pg. 231 e 232.
[53] FERNANDO GONÇALVES, MANUEL MONTEIRO GUEDES VALENTE, JOÃI MANUEL ALVES, *O novo regime jurídico… Op. Cit.* Pg. 37; *Idem*, *Lei e Crime: O agente infiltrado versus o agente provocador. Os princípios do processo penal.* Coimbra: Almedina. 2001. Coimbra: Editora Almedina. 2001. Pg. 256; Também neste sentido se posiciona Germano Marques da Silva, de acordo com o qual "(…) a provocação não é apenas informativa, mas é formativa; não releva o crime e o criminoso, mas cria o próprio crime e o próprio criminoso. A provocação, causando o crime, é inaceitável como método de investigação criminal, uma vez que gera o seu próprio objecto". *Cfr*. GERMANO MARQUES DA SILVA, *Curso de Processo Penal* – Vol. II, 5ª Edição, revista e actualizada. Lisboa: Edição Babel, 2011. Pg. 233.
[54] CRISTINA DE MAGLIE, *L'Agente Provocatore – Un'indagine dommatica e politicocriminale*, Milano, Milano - Dott. A. Giuffrè Editore, 1991. Pg. 359.

provocador instiga o sujeito a cometer o crime, mas não quer que o crime se consuma", faltando, portanto, a segunda conexão de vontade necessária para a atribuição do facto por dolo ao agente provocador".[55]

Alves Meireis, apoiando-se nos argumentos de Cristina Maglie, vem do mesmo modo definir os agentes provocadores como "aqueles que, sendo agentes da autoridade ou cidadãos particulares a actuar concertadamente com os primeiros, e aproveitando-se de uma certa predisposição do suspeito para o crime, o convencem à sua prática, não querendo o crime a se, e, sim, pretendendo submeter esse outrem a um processo penal e, em último caso, a uma pena".[56] Na perspetiva do autor, ao agente provocador não poderá ser reconhecido qualquer dolo de consumação, na medida em que, não querendo que o crime aconteça em si mesmo, apenas se limita a convencer alguém à prática de atos que permitam com muita probabilidade identificar uma intenção criminosa suficientemente notória para servir*, a posteriori*, de fundamento "a um processo penal e, em último caso, a uma pena"[57].

Em termos semelhantes, Duarte Rodrigues Nunes aponta como critério diferenciador entre o agente provocador e o encoberto o facto de o primeiro apresentar uma nítida intenção de despoletar a prática do crime e o segundo se limitar a acompanhar um crime já estava pré-decidido pelo criminoso.[58].

Last but not least, cumpre-nos também mencionar que não se confundem com o agente encoberto e/ou infiltrado as figuras do informador, do arrependido e do mero denunciante anónimo.[59]

---

[55] *Ibidem*. Pg. 360.

[56] MANUEL AUGUSTO ALVES MEIREIS, *O Regime das Provas… Op. Cit.* Pg. 163.

[57] *Ibidem*. 1999. Pg. 97.

[58] Não obstante, admitindo que a diferença entre as figuras possa ser ténue, aponta alguns critérios de que nos podemos socorrer para as distinguir, mormente: os antecedentes criminais do suspeito relativos a crimes similares, a predisposição para a prática do crime, o fundamento e grau de suspeita sobre o visado e a intensidade, género e objetivo da influência exercida sobre o visado. *Vide:* DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade… Op. Cit.*. Pg. 837.

[59] Será um mero informador "aquela pessoa cujos dados são reservados, e que, confidencialmente, fornece material informativo acerca de delitos, prestando uma valorosa ajuda aos funcionários de investigação criminal"; já o arrependido corresponderá ao "indivíduo que, pertencendo originalmente à organização criminosa, a partir de certo momento (em troca de certos benefícios legais e de protecção), colabora com as autoridades judiciárias (…)"; e, finalmente, o denunciante anónimo será "um particular que leva ao conhecimento das autoridades a notícia da efectivação de crimes e que, aos poucos, lhes vai transmitindo algum elemento probatório de relevância." (*Cfr.* PAULO PINTO DE SOUSA, *Acções Encobertas. Meio enganoso de prova? Agente infiltrado e agente provocador. Outras questões*, in Revista do CEJ, Editora Almedina, 2010. Pg 234 e 235). Susana Aires de Sousa esclarece que enquanto o agente encoberto "é um interveniente processual previsto na lei processual penal e a sua atuação constitui um meio de obtenção de prova", o informador, contrariamente, "não tem qualquer estatuto processual e a informação por si prestada é

2.2. A ação encoberta física e a ação encoberta digital - aspetos em comum e aspetos diferenciadores conducentes a uma (não) equiparação das suas realidades

As ações encobertas digitais, modalidade de ação encoberta sobre a qual nos debruçamos com maior afinco no nosso estudo, não encontram hoje um espaço de regulamentação próprio. De facto, o legislador processual penal considera a mera remissão por analogia para o RAJE – a Lei nº101/2001 de 25 agosto –, compensada apenas pelo art. 19º da LC - a Lei nº 109/2009 de 15 de setembro -, o raciocínio e operação bastantes para a sua regulamentação.

Sucede que, como bem elucida David Silva e Ramalho, "(…) a redução de uma realidade complexa a um núcleo simples, vago e abstracto, com o objetivo de nele e*ncaixar* uma realidade semelhante mas com diferenças relevantes, é susceptível de revelar insuficiências ao nível da densificação, do detalhe e da regulamentação específica de aspectos diferentes decorrentes da natureza dos contextos respectivos."[60] Uma tal asseveração pode, desde logo, ser feita se atentarmos às diferenças que a ação encoberta física e a ação encoberta digital apresentam ao nível do seu *modus operandi,* riscos envolvidos e custos da operação. Vejamos:

1) Enquanto na ação encoberta física o agente encoberto pode, quando muito, beneficiar da possibilidade de lhe ser atribuída uma identidade fictícia física que deverá manter (tal e qual como fora autorizada) para atuar e contactar com o meio criminoso, o agente encoberto digital pode, numa mesma ação e simultaneamente, utilizar diferentes facetas e identidades fictícias, consoante o momento e o estádio em que se encontre a investigação. Assim, é perfeitamente possível que o agente encoberto digital possa assumir, concomitantemente, a faceta de criminoso e a de potencial vítima. Tal sucederá, a título de exemplo,

processualmente irrelevante" *(Cfr.* SUANA AIRES DE SOUSA, *Ações encobertas (e outras figuras próximas) na investigação da criminalidade económico-financeira in* Revista Julgar nº 38. maio/agosto de 2019. Pg. 39). Isabel Oneto alerta ainda para o facto de ser relativamente comum o recurso a informadores por agentes encobertos. Efetivamente, um dos grandes comportamentos desviantes do agente encoberto relaciona-se com a proteção dos informadores que, estando inseridos no seio criminoso, aceitam, a troco de dinheiro ou de uma garantia, contribuir para a recolha de material probatório. Tal posição de domínio dos agentes sobre os seus informadores revela-se preocupante, na medida em que "acaba por permitir a construção de uma teia de relações à margem do sistema e coloca dificuldades logo ao nível da observância do princípio da oportunidade e da igualdade". *Cfr.* ISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 92 e 93.

[60] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit*. Pg. 284.

quando o agente se faça passar, numa das salas virtuais, por vendedor de material ilícito, e, noutra, por comprador; ou ainda, como exemplifica David Silva Ramalho, quando se faça passar por um pedófilo numa das salas e noutra por um menor de idade, potencial vítima.[61] Por outro lado, o agente encoberto digital pode ainda ir mais além na sua forma de atuação: poderá assumir não uma identidade fictícia, mas a identidade de um eventual criminoso ou de uma pessoa da confiança dos investigados, o que é possível mediante a apropriação da sua conta de utilizador.[62] Através dessa apropriação o agente poderá ter acesso a informações, declarações e outras confidências relativamente aos crimes investigados. Note-se que nas ações encobertas físicas muito dificilmente um agente consegue fazer-se passar por alguém que seja da confiança de um dos potenciais criminosos investigados.

2) Enquanto a ação encoberta física se desenvolve num espaço físico propriamente dito – um bar, uma discoteca, um restaurante -, onde o agente se mantém a generalidade das vezes lado-a-lado com os potenciais criminosos investigados ou até mesmo interage com eles, a ação encoberta digital para ter sucesso não carece necessariamente de um qualquer contacto, interação ou comunicação. De facto, é perfeitamente possível que ela se realize no âmbito de "websites públicos ou privados, nos quais os participantes comunicam somente através de comentários em fotografias"[63] ou no âmbito de "mercados negros digitais como o *Silk Road* em que a interação entre compradores e vendedores de produtos ilícitos é mínima e tendencialmente não implica qualquer comunicação".[64] Note-se que mesmo as ações encobertas digitais que se desencadeiam no âmbito das redes sociais e em que possa ser necessária a criação de amizades virtuais e em que existe, portanto, uma maior interação entre agente/investigado, esse grau de interação em nada se compara àquele é exigido numa ação encoberta física.
3) O facto de o agente encoberto digital se "esconder" por detrás de um aparelho eletrónico determina menores riscos para a sua segurança. Enquanto o agente encoberto digital pode realizar a sua investigação sem ter que se deslocar

[61] *Ibidem*. Pg. 284.
[62] *Ibidem*. Pg. 285.
[63] *Ibidem.* Pg. 285.
[64] *Ibidem.* Pg. 285.

fisicamente ao lugar da prática do crime e expor a sua imagem, o agente encoberto físico não o poderá fazer. De facto, não podemos equiparar os esforços e riscos da operação do agente encoberto físico com os do agente encoberto digital: enquanto o primeiro terá que, muitas das vezes, se deslocar para lugares longínquos, perigosos e fora da sua zona de conforto para poder produzir prova, o agente encoberto digital poderá manter-se resguardado no seu escritório (muitas das vezes localizado na sua própria casa), bastando-lhe vaguear por *websites* ou salas *online* onde os crimes decorrem. E note-se bem: mesmo que haja um imprevisto que possa colocar em causa o sucesso da operação, a sua segurança não fica, por regra, comprometida. Numa ação encoberta física sabemos que qualquer "passo em falso" poderá não só determinar o insucesso da operação, mas também e, essencialmente, a colocação em risco da própria segurança do agente.[65] A sua revelação poderá ter como consequência a impossibilidade de o agente poder voltar a atuar nessa condição em casos futuros (o que, numa perspetiva de rentabilização de recursos, não será eficiente, dado não haver certamente muitos agentes ou terceiros especialmente preparados e treinados para assumir essas funções junto dos Departamentos de Polícia); e, sobretudo, mais importante, o facto de a sua revelação poder ter como consequência máxima indesejável a colocação do agente em risco sério de vida, assim como dos seus familiares e/ou amigos mais próximos. Ademais, a necessidade de se recorrer a uma identidade fictícia não é tão essencial como o é nas ações encobertas clássicas, podendo até mesmo ser dispensada em determinados casos.[66]

4) Também ao nível da facilidade de recolha de prova, as ações encobertas físicas apresentam limitações mais notórias: o agente encoberto estará confinado à sua perceção sensorial, na exata medida em que a prova que poderá obter será o resultado daquilo que possa ver ou ouvir. Ora, se pensarmos na possibilidade de o agente encoberto se encontrar a atuar num espaço barulhento, com uma grande multidão, naturalmente terá sérias dificuldades em ver ou ouvir. Já em ambiente digital essa tarefa estará, em princípio, facilitada porquanto o agente tem um

[65] *Ibidem.* Pg. 285.
[66] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 74.

acesso privilegiado a toda a informação, não estando limitado por obstáculos físicos que impeçam o seu contacto sensorial com a prova. Note-se que, como evidencia David Silva Ramalho, o agente poderá nem sequer estar à frente do computador durante a atividade investigativa, podendo simplesmente limitar-se a gravar tudo o que é dito num *chat* ou a registar o que acontece num *website*.[67] Por outro lado, a benesse de o agente encoberto digital poder frequentar paralelamente distintos espaços virtuais, com recurso a diferentes personalidades criadas para o efeito ou já existentes, torna a tarefa da obtenção de prova mais fácil.

5) Uma outra diferença de relevo é também o modo de comunicação e interação entre os suspeitos investigados. De facto, quando em causa está uma interação digital a partir de redes sociais, fóruns, *chats, blogs* ou *websites*, os intervenientes, por regra, não partilham a sua verdadeira identidade, recorrendo antes a *usernames* ou *nicknames.* Assim, diferentemente do que acontece em ambiente físico, em que os intervenientes interagem pessoalmente, em ambiente digital "a ocultação de identidade é a regra perante todos, sendo a identificação pessoal a excepção."[68]
6) Também o elevado poder que o agente encoberto digital detém, derivado dos conhecimentos técnico-científicos que possui e das ferramentas técnicas inerentes à computação que o próprio método oculto de investigação lhe proporciona, comporta um risco que não assistimos existir na ação encoberta física: "o do aproveitamento, por parte do agente encoberto, do acesso privilegiado ao visado e das tecnologias anti-forenses à sua disposição para benefício próprio (praticando ilícitos não relacionados com a acção encoberta), ou em benefício ilícito da investigação (promovendo a prática de crimes com uma identidade fictícia e recolhendo prova com outra)".[69] Estes riscos implicam que haja um "dever acrescido de controlo por parte da autoridade judiciária e uma obrigação de registo permanente de toda a actividade empreendida pelo agente no decurso da ação".[70]

[67] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 295 e 296.
[68] *Ibidem.* Pg. 293.
[69] *Ibidem.* Pg. 286.
[70] *Ibidem. Pg. 286.*

7) As ações encobertas digitais acarretam o emprego de menores esforços, na medida em que as atividades do agente podem ser realizadas por diversos OPC, em comunhão de esforços, bastando apenas o conhecimento dos factos e a utilização do mesmo tipo de linguagem para se evitar que os sujeitos investigados se apercebam de que com eles interagem pessoas diferentes.[71] A atuação de vários agentes torna a ação encoberta menos cansativa e poderá conduzir a resultados mais rápidos e eficientes em função do trabalho em equipa multidisciplinar.[72]
8) Por outro lado, também não podemos deixar de reconhecer que a versão digital da figura permite a posse e preservação de um registo eletrónico de todas as ações do agente que, em caso de dúvidas ou eventuais vicissitudes legais, possibilitará o desencadeamento de uma perícia que permita demonstrar as especificidades da sua atuação.[73]
9) Também numa perspetiva económico-financeira, facilmente se compreende que uma ação encoberta física poderá acarretar maiores custos-financeiros para o Estado relativamente àqueles que uma ação encoberta digital exige: pense-se nas hipóteses que em o agente encoberto físico, para poder investigar "no terreno" e, eventualmente, produzir prova, terá que se deslocar para o lado oposto do país onde se encontra, ou até mesmo para outro país, juntando-se às despesas de deslocação as de estadia, alimentação, bem como outras inerentes à própria investigação. Efetivamente, numa ação encoberta digital essas despesas estão, por norma, excluídas: segundo F. Bueno de Mata para que a ação se torne operativa basta um equipamento informático atualizado, a conexão a uma rede de Internet e um funcionário das forças de segurança do Estado.[74]
10) Finalmente, mas não menos importante, nas ações encobertas digitais que se desenrolem com recurso a *benware* poderá nem sequer ser necessária a

[71] *Ibidem.* Pg. 74.
[72] *Ibidem.* Pg. 87.
[73] MARCELO TEMPERINI, MAXIMILIANO MACEDO, *Nuevas Herramientas… Op. Cit.* Pg. 512.
[74] De acordo com o Autor "el establecimiento de esta figura [del agente encubierto digital] desde el punto de vista del coste económico no sería problemático, puesto que no supondría ningún desembolso de dinero para las arcas del Estado." *Cfr.* FEDERICO BUENO DE MATA, *El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia*, in Actas del IV Congreso Galego de Derecho Procesal (I internacional), A Coruña, 117 2 y 3 de junio de 2011. Pg. 302 e 305.

> intervenção de qualquer agente encoberto, na exata medida em que, como veremos mais momento ulterior mais oportuno, é o próprio *software* que efetua autonomamente a recolha de prova digital[75], prova essa que se distingue igualmente da prova física, desde logo, pela sua imaterialidade ou invisibilidade.[76]

As diferenças contrastantes entre a investigação no meio digital e no meio físico evidenciadas poderão constituir os primeiros indícios de que a mera adaptação e aplicação das regras previstas no RJAE, pensadas e criadas à luz das especificidades do mundo físico, ao mundo virtual poderá não só ser insuficiente como também perigoso. Ora, indagar se o raciocínio analógico a que se tem apelado entre as duas realidades será razoável implica que analisemos se o RAJE, corporizado na Lei nº 101/2001 de 25 de agosto, analogicamente aplicado, e compensado unicamente pelo art. 19º da LC, materializado na Lei nº 109/2009 de 15 de setembro, é capaz de responder eficientemente aos problemas que as ações encobertas digitais convocam.

[75] Neste sentido avança ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 74.
[76] *Cfr.* SÓNIA FIGALDO, *A utilização de inteligência artificial… Op. Cit.* Pg. 134.

PARTE II: REGIME JURÍDICO VIGENTE DAS AÇÕES ENCOBERTAS DIGITAIS – "AS LEIS QUE TEMOS"[77]

3. A Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro) – em particular, o art. 19º

«A Lei nº 109/2009 de 15 de setembro veio aprovar a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.»[78]

Este Diploma assume-se como um verdadeiro marco na história jurídica portuguesa na medida em que, inspirado na Recomendação n.º R (89) 9 do Conselho da Europa, de 13 de setembro, veio substituir e revogar a velha Lei da Criminalidade Informática – a Lei nº 109/91 de 17 de agosto -, já francamente desadaptada à realidade tecnológica dos dias de hoje, adaptando as regras processuais ao mundo virtual. Incidindo sobre disposições penais materiais e processuais, bem como sobre as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, não se descurou de fazer referência ao método oculto de investigação criminal sobre o qual nos debruçamos na presente dissertação.

Deste modo, a Lei do Cibercrime veio, assim, proceder ao alargamento das ações encobertas à cibercriminalidade, formalizando uma nova espécie de atuação encoberta no seu art. 19º, de tal forma que, nas palavras de Susana Aires de Sousa, "a par do agente encoberto físico, deve hoje enunciar-se a ação encoberta digital ou eletrónica"[79].

Tal preceito, "uma originalidade que não decorreu de qualquer previsão da Convenção do Conselho da Europa, nem da Decisão-Quadro[80]", e que tem como epígrafe "acções encobertas", permitiu a ampliação do âmbito de aplicabilidade deste método oculto de investigação criminal que até então se encontrava cingido ao art. 2º do RJAE, admitindo-

[77] Título inspirado no texto: JOÃO CONDE CORREIA, *Prova digital: as leis que temos e a lei que devíamos ter, in* Revista do Ministério Público, Ano 35, nº 139, julho-setembro, 2014.
[78] Sumário da Lei nº 109/2009 de 15 de setembro.
[79] SUSANA AIRES DE SOUSA, *Ações encobertas… Op. Cit.* Pg. 33 e 34.
[80] PAULO DÁ MESQUITA, *Processo Penal, prova e sistema judiciário,* Coimbra: Coimbra Editora. 1ª Edição, setembro de 2010. Pg. 126.

se agora a admissibilidade do recurso às ações encobertas digitais, no decurso do inquérito, no âmbito dos seguintes crimes:

"i) [dos] *previstos na presente lei* [nos arts. 3º a 8º da Lei nº 109/2009 e outros que venham a ser introduzidos no Diploma];

ii) [d]*os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e*

iii) sendo dolosos, [independentemente da pena aplicável], [dos] *crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes,* [d]*a burla qualificada,* [d]*a burla informática e* [d]*as comunicações,* [d]*a discriminação racial, religiosa ou sexual,* [d]*as infracções económico financeiras, bem como* [d]*os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos."*

Ora, embora o preceito possa parecer simplista, a verdade é que não reúne consenso. Se, por um lado, se revela inovador por abrir caminho à regulamentação das ações encobertas em ambiente digital, por outro, continua a ser vago e impreciso, pois limita-se a remeter a regulação das ações encobertas digitais para o RAJE, um regime que foi idealmente pensado para um modo de investigação que se desenrola em ambiente físico, e não se dignou a concretizar quais e em que medida poderão ser utilizados os meios e dispositivos informáticos na realização da ação encoberta.[81] De facto, muito se tem questionado se esta técnica legislativa com a manutenção da predominância processual penal para o espaço físico, compensada apenas pela aplicação das regras do regime geral das escutas telefónicas previstas no art. 189º do CPP e da interceção de comunicações previstas no artigo 18º da Lei do Cibercrime, para todo o tipo de comunicação (telefónica ou digital), será suficiente no âmbito de um modo de investigação com especificidades sensivelmente diferentes.[82]

Ora, em face do exposto, Armando Dias Ramos avança que da opção legislativa "resultou inequivocamente uma confusão de conceitos diferentes numa só situação", com o encaixe da utilização ativa de um agente encoberto digital e da interceção de comunicações

[81] Também neste sentido: SUSANA AIRES DE SOUSA, *Ações encobertas… Op. Cit.* Pg. 38.

[82] Note-se que um tal questionamento acaba por se intensificar quando pensamos que neste método oculto de investigação criminal os elementos recolhidos pelo agente tornam-se, por regra, prova de crimes já consumados, não havendo clareza no que toca à possibilidade de serem prosseguidas finalidades preventivas, repressivas ou ambas em simultâneo. *Cf. Ibidem*. Pg. 38.

em dispositivos informáticos numa única situação, "duas realidades distintas que são incompatíveis quer do ponto de vista dos métodos de obtenção de prova, quer nos distintos regimes processuais em vigor".[83]

Ademais, aponta-se ainda que, olhando para outros ordenamentos jurídicos, é claro o atraso do nosso ordenamento na regulação das questões em matéria de cibercriminalidade: veja-se, a título de exemplo, o ordenamento jurídico italiano que, ao invés de se limitar a fazer meras remissões legislativas, dispersas entre si (como se faz entre nós em matéria de ações encobertas), procurou por alterar o seu próprio Código de Processo Penal, introduzindo novas disposições processuais aptas a dar resposta aos novos meios de obtenção de prova.[84] Diferentemente, a legislação portuguesa sobre cibercriminalidade acaba por ser apenas o resultado da transposição de diretivas, decisões-quadro e outros diplomas oriundos das instâncias europeias, em atos isolados e dispersos (por exemplo, a LC é um decalcamento da Ciberconvenção e da Decisão-Quadro nº 32/2008, de 17 de julho e da Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro), como se, nas palavras proferidas por Paulo Dá Mesquita, de uma verdadeira "*manta de retalhos*" se tratasse.[85]

Efetivamente, a dispersão legislativa a que assistimos existir na regulamentação da nossa cibercriminalidade, agravada pela aplicação de um regime geral previsto em lei extravagante, deixa muito a desejar. Note-se que o legislador, com a criação da Lei do Cibercrime, não revogou as outras normas do CPP que lhe antecediam. Assim, embora a doutrina maioritária considere que os Diplomas se complementam[86], a verdade é que nem por isso deixam de se confrontar em determinadas matérias.

Olhando o art. 19º da LC, preceito que releva para nós, como bem evidencia David Silva Ramalho, "a norma apresenta-se, numa primeira leitura, como uma mera adição de certos crimes informáticos (*stricto sensu*) ou cometidos através de um sistema informático ao catálogo previsto no art. 2º da Lei nº 101/2001, para efeitos do recurso às acções encobertas aí previstas e «nos termos aí previstos»[87]. De facto, parece-nos que o legislador

---

[83] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 18.
[84] PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 98.
[85] *Ibidem*. Pg. 111.
[86] Na qual se incluem Autores como, por exemplo: RITA CASTANHEIRA NEVES, *As ingerências nas Comunicações Electrónicas em Processo Penal, Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, 1ª Ed., Coimbra: Coimbra Editora, 2011. Pg. 234 e ss.
[87] DAVID SILVA RAMALHO, *Métodos ocultos... Op. Cit.* Pg. 303. No mesmo sentido, SAUSANA AIRES DE SOUSA, *Ações encobertas… Op. Cit.* Pg. 37.

ficou "a meio caminho" naquilo que seria o preenchimento de uma lacuna que há algum tempo tem vindo a ganhar protagonismo: a regulamentação das ações encobertas em ambiente digital. Note-se que esta insuficiência legislativa poderá, desde logo, ser percecionada pelo facto de norma se limitar a ampliar o catálogo de crimes, nada prevendo quanto aos específicos meios e dispositivos informáticos subjacentes às atividades do agente encoberto digital e, como nota Paulo Dá Mesquita, aos termos de "ocultação da qualidade e identidade" em interações comunicacionais no quadro das redes eletrónicas.[88]

Observando o nº 2 do mesmo preceito, nele se estipula que "*sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.*" Ora, assistimos aqui, uma vez mais, à manutenção da mesma técnica de regulação por remissão, na exata medida em que o legislador continua a limitar-se a remeter a regulação das ações encobertas digitais para outros métodos de investigação já com um espaço próprio de regulamentação no CPP, ínsito nos artigos 187º a 189º, não especificando o que se entende por "recurso a meios e dispositivos informáticos", nem em que medida tal se tal operará.

Como refere David Silva Ramalho, a formulação vaga da disposição, introduzida como última norma do regime processual penal em matéria de prova digital e sistematicamente inserida num artigo relativo a uma figura jurídica utilizada em casos excecionais, determinou a sua desconsideração junto da doutrina, na medida em que continua a ser encarada apenas como uma norma que visa facultar aos OPC meios técnicos indefinidos, análogos à interceção de comunicações, no âmbito das ações encobertas digitais. Porém, alerta o autor para o facto de, na verdade, esta norma poder trazer consigo implícita uma consequência importante: o nascimento de um novo meio oculto de obtenção de prova.[89]

De facto, a necessidade sentida pelo legislador em introduzir uma norma nova para legitimar o recurso a estes "meios e dispositivos informáticos", em face da insuficiência da utilização dos restantes meios processuais existentes consagrados na legislação processual penal portuguesa, confirma a novidade deste meio. Note-se que a própria letra da lei acaba

[88] PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 126.
[89] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 344.

por apontar para a sua originalidade, ao remeter o intérprete apenas "*naquilo que foi aplicável*" para o regime da interceção de comunicações. [90]

Entre nós, no que a esta possibilidade respeita, entendemos, numa primeira análise, que a não subsunção destes "meios e dispositivos informáticos" a qualquer um dos meios de obtenção de prova já consagrados acaba por se impor até pela natureza das coisas. Atendendo à definição de agente encoberto patente no RAJE, parece-nos que a recondução da ação encoberta digital a uma mera interceção de comunicações seria redutora, na medida em que as atividades do agente encoberto são complexas e abrangem uma grande variedade de formas específicas de investigação, que não podem ser cingidas à simples interceção de comunicações.[91]

Resta-nos, deste modo, decifrar a que "*meios e dispositivos informáticos*" o legislador se refere, questão que, mesmo com a alteração à LC em 2021, operada pela Lei nº 79/2021 de 24 novembro, continua por resolver.[92]

---

[90] DAVID SILVA RAMALHO, *O uso de malware como meio de obtenção de prova em processo penal, in* Revista de concorrência e regulação - C&R. ISSN 1647-5801. Ano 4, n.º 16, 2013. Pg. 230.

[91] De relevar ainda que a referência a estes "meios e dispositivos informáticos" – não reconduzíveis aos dispositivos eletromagnéticos, acústicos, mecânicos ou outros comummente utilizados nas interceções nos exatos termos do art. 2º/ e) da LC - poderá ser ainda a responsável pela consideração das ações encobertas digitais como um "meio particularmente gravoso de investigação". Efetivamente, como bem elucida o preceito, o recurso a estes meios e dispositivos informáticos encontra-se limitado ao contexto excecional das ações encobertas digitais. Assim, a norma ao sublinhar expressamente a sujeição deste método de obtenção de prova (que, à partida, já se sabe de antemão que exige cautelas especiais pela sua excecionalidade), aos critérios da necessidade e da subsidiariedade parece indiciar que se tratará de um meio com um grau de lesividade e devassa superior às próprias ações encobertas tradicionais. *Cfr*. *Ibidem*. Pg. 230 e 231.

[92] De acordo com Armando Dias Ramos, daquela alteração resultou apenas a introdução de novos artigos na Lei do Cibercrime, referente aos crimes relacionados com a fraude e a contrafação de meios de pagamento que não em numerário, com a ampliação do catálogo crimes relativamente aos quais será admissível a realização de ações encobertas. C*fr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 246. Não foi feita, portanto, qualquer referência ao próprio *modus operandi* do agente encoberto digital, pelo que as mais recentes alterações legislativas nesta matéria continuam a revelar-se incapazes de resolver os problemas associados a este método oculto de investigação criminal.

4. O Regime Jurídico das Ações Encobertas para fins de prevenção e investigação criminal (Lei nº 101/2001 de 25 de agosto)

O RJAE, vertido na Lei nº 101/2001 de 25 de agosto, veio revogar as normas existentes até à data, dando-nos uma primeira noção explícita de ações encobertas, no nº 2 do seu art. 1º, que passamos a citar:

"Consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados neste diploma, com ocultação da sua qualidade e identidade".

Numa primeira análise denotamos que a Lei permite que as ações encobertas sejam levadas a cabo por funcionários de investigação criminal[93] ou por terceiro, de forma indiscriminada. Da norma não resulta, portanto, que OPC ou terceiros podem, em concreto, figurar como agente encoberto, nem sequer quais os processos da sua seleção e formação.

Como evidencia Dias Ferreira, citada por Isabel Oneto, a definição desse processo de seleção afigurar-se-ia essencial, na medida em que configura "uma primeira garantia" contra o (eventual) fracasso das operações do agente encoberto.[94] De maneira que, tal como sucede junto do FBI e das polícias locais norte-americanas, deveriam ser estipulados, nos termos da lei, níveis de seleção, traduzidos na necessidade de, em concreto, o aspirante a agente encoberto apresentar "capacidade física e psicológica", de "improviso face a situações inesperadas", de "manipulação e de representação", "estabilidade familiar" e

[93] Para sustentar a sua tese, o Autor socorre-se do exemplo, no âmbito do processo de inquérito 13/10.4GAPNF, da decisão proferida pelo JIC da nulidade das provas obtidas contra os arguidos que assaltaram um cofre nas bombas de combustível da Rebordosa, em Paredes, porque obtidas pela GNR, por ter atuado como se pudesse assumir as vestes de um agente encoberto, quando tal possibilidade lhe estava vedada. Acrescenta ainda o Autor que com a legislação atual também o caso *Teixeira de Castro vs Portugal* não chegaria às instâncias do TEDH, justamente por não ser permitida a atuação da PSP ao abrigo do RJAE. *Vide:* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.*. Pg. 69. Também neste sentido: FERNANDO GONÇALVES, MANUEL MONTEIRO GUEDES VALENTE, JOÃO MANUEL ALVES, *O novo regime… Op. Cit.* Pg. 42; *Idem, Lei e Crime: O agente infiltrado versus o agente provocador… Op. Cit.* Pg. 276; Contra este entendimento se apresenta Isabel Oneto, de acordo com a qual "o que a lei pretende dizer (…) é que a direcção da operação, sem prejuízo das necessárias autorizações das entidades judiciárias, compete à Polícia Judiciária, actuando esta com autonomia técnica e táctica", na medida em que "não faria sentido que um terceiro, estranho a qualquer força policial, pudesse ser agente infiltrado, negando-se depois essa possibilidade a um agente de outra força policial que não a Polícia Judiciária." *Cf.* ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 142.

[94] VANESSA P. DIAS FERREIRA, *Problèmes Posés par la Mise em Oevre des Opérations Undercover dans les Domaine de la Lutte contre le Trafic de Stupéfiants in* Révue de droit Penal et de Criminologie, ano 76, Bruxelas, 1996, Pg. 562 *Apud* ISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 84.

"motivação para o exercício daquela função".[95] Neste sentido, Paulo Pinto de Sousa aponta que o legislador penal se possa ter excedido na delimitação do seu âmbito subjetivo ativo, na medida em que, na sua ótica, em causa estão atividades que só poderiam dever ser exercidas por quem tivesse sido alvo de uma preparação exigente, capaz de fornecer as competências especializadas necessárias para tal.[96]

De facto, atendendo à possibilidade introduzida pela letra da lei em serem levadas a cabo ações encobertas por um terceiro, isto é, por um qualquer cidadão particular, sem serem especificados os critérios da sua escolha, este método de investigação corre o risco de vir a relevar-se dúbio e perigoso: primeiro, pela sua maior vulnerabilidade e tendência para a sua corrupção e, em segundo, porque, por regra, não possuem as capacidades psicológicas e físicas para fazer face aos elementos que penetram na estrutura das organizações criminosas, além da necessária experiência no trato com o mundo do crime.[97] Note-se que, como evidencia Maria de Sousa, tendo sido deixado ao livre critério da PJ a escolha do agente encoberto, sem sequer ter sido limitada a qualidade do terceiro, tal poderá ter como consequência máxima indesejável a assunção do papel de agente encoberto por indivíduos que se encontram a ser alvo de uma investigação, com cadastro criminal ou até mesmo a cumprir uma pena[98], circunstância que nunca poderá verificar-se num processo penal que se pretende o mais eficaz e justo possível.

Ora, entre nós, embora esta possibilidade de recurso a terceiros no âmbito de uma ação encoberta seja criticável, não podemos deixar (pelo menos do ponto de vista teórico) de lhe atribuir sentido, bem como não podemos negar que, por vezes, constitui a medida mais idónea quando pensada numa perspetiva de eficiência da justiça criminal. Pense-se, nomeadamente, em situações em que, como exemplifica David Silva Ramalho, em causa esteja um terceiro integrado no meio criminoso ou cujos especiais conhecimentos técnicos lhe permitam infiltrar-se em áreas que, de outro modo, permaneceriam inacessíveis a agentes

---

[95] *Cfr.* ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 85.

[96] Sandra Pereira aponta que a "questão dúbia nesta disposição [se] prende com a possibilidade de ser alguém de fora das estruturas vocacionadas para a investigação criminal a actuar enquanto agente encoberto" e que "a utilização de terceiros pode acarretar dificuldades acrescidas". (SANDRA PEREIRA, *A recolha de prova… Op. Cit.* Pg. 150). Note-se que, diferentemente, no ordenamento jurídico espanhol, atento o nº 6 do art. 282º da LECrim, apenas funcionários da PJ estão legitimados a encetar ações encobertas digitais.

[97] PAULO PINTO DE SOUSA, *Acções Encobertas… Op. Cit.* Pg. 233 e 234.

[98] MARIA CLARA DE FREITAS MORNA ALVES DE SOUSA, *O Agente Infiltrado No Ordenamento Jurídico Português,* Dissertação de Mestrado. Faculdade Direito da Universidade Coimbra. Coimbra. 2012. Pg. 87.

encobertos da polícia.[99] Nestes casos, Armando Dias Ramos considera que não seja inconstitucional a recolha de elementos probatórios por esses terceiros, desde que sejam respeitados os mesmos princípios a que deve obedecer uma ação encoberta realizada por um funcionário de polícia criminal.[100] Sandra Pereira acrescenta ainda que a utilização de terceiros deve ser controlada e fundamentada, devendo ser explicitado o motivo pelo qual existe preferência por esse terceiro e não por um agente de autoridade, evitando, desse modo, "situações ilegais de promiscuidade e de falta de transparência nessas operações".[101]

Na nossa perspetiva, embora não discordemos com a participação de terceiros na ação encoberta, entendemos que o grande problema reside na possibilidade em figurar como terceiro um eventual (co)arguido, caso em que existem dúvidas quanto a saber se a assunção desse papel será compatível com o seu estatuto processual. David Silva Ramalho parece admitir esta possibilidade apoiando-se no argumento de que, nesse caso, todas as declarações que o terceiro venha a prestar serão feitas enquanto coarguido, nos exatos termos do art. 345º/4 CPP, e não como testemunha, isto é, ao abrigo do art. 133º/1/a) CPP, pelo que não se corre o risco processual de vir a participar com o mero objetivo de se ilibar da responsabilidade criminal que sempre lhe caberia.[102] Ora, entre nós, embora seja verdade que nesse caso o terceiro sempre fosse chamado à responsabilização criminal, a grande questão é que, participando na ação encoberta, também não poderá deixar de beneficiar dos direitos processuais atribuídos pela lei processual portuguesa enquanto (co)arguido, entre os quais o direito a recusar-se a prestar declarações sobre as investigações que tenha feito em sede de audiência de julgamento[103], o direito ao silêncio[104] e à não autoincriminação, o que pode prejudicar o apuramento da verdade dos factos e o sucesso das investigações. Embora contra este argumento sempre se pudesse dizer que esta desvantagem acaba por ser, em certa medida, ultrapassada pelo facto de, em ambiente digital, a prova produzida ser sustentada maioritariamente por ficheiros, documentos, bases de dados, não sendo a participação e declarações do agente na audiência tão premente quanto será no âmbito de uma ação encoberta física, não deixa aquele facto de ser um obstáculo ao bom andamento do processo.

[99] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 299.
[100] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit*. Pg. 63.
[101] SANDRA PEREIRA, *A recolha de prova… Op. Cit.* Pg. 152.
[102] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 300.
[103] *Cfr.* Art. 343º do CPP.
[104] *Cfr.* Art. 61º, nº1, al. d) do CPP.

De maneira que, na nossa ótica, o grande problema não reside na possibilidade de nas investigações poderem participar terceiros. A questão deverá antes centrar-se na eventualidade em serem os próprios (co)arguidos a levar a cabo, em sentido material, a investigação. De facto, tal como nos elucida David Silva Ramalho, atendendo ao contexto em que as ações encobertas digitais se desenrolam, todo o (co)arguido que pretenda efetivamente colaborar com a justiça, não tendo por detrás qualquer outra intenção duvidosa, poderá fazê-lo facultando voluntariamente as suas credenciais de acesso aos "locais" da prática criminosa, às forças policiais que, por sua vez, assumindo ficticiamente a sua identidade, procurarão produzir prova.[105] Deste modo, se nas ações encobertas físicas esta participação ativa do (co)arguido enquanto agente encoberto poderá revestir algum fundo de sentido (se é que reveste), nas ações encobertas digitais deixa de assumir, em função da própria natureza das investigações, não se afigurando sequer necessária a assunção pelo terceiro (co)arguido do papel de agente encoberto em ambiente digital.

Feitas estas considerações, está, assim, reunido um conjunto de argumentos bastante para indagar que a definição constante do art. 1º/2 do RJAE não só não está suficientemente densificada por dela não ser possível o apuramento do processo de seleção, formação e supervisão dos agentes encobertos (garantidor do sucesso da operação)[106], como não responde eficientemente ao modo e em que condições o agente encoberto digital poderá atuar caso seja um terceiro, eventual (co)arguido.

4.1. Âmbito de aplicação

Explicitada a definição de ação encoberta que convoca, desde logo, como vimos, algumas interrogações, o legislador prossegue no art. 2º do RJAE com a identificação do conjunto de crimes em relação aos quais este método de investigação criminal pode ser utilizado, reconhecendo-o como um importante recurso "no âmbito da prevenção e repressão"[107] criminais. Deste modo, uma análise atenta ao preceito permite-nos verificar que o legislador procurou alargar o âmbito de aplicação das ações encobertas, na medida em que deixou de as circunscrever aos crimes económico-financeiros e relacionados com o

[105] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 300.
[106] ISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 84.
[107] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 300.

tráfico de estupefacientes para passar a prevê-las também relativamente a outro tipo de criminalidade.

Hoje é de entendimento pacífico que, apesar de constituir um método de investigação criminal eficaz na luta contra a criminalidade organizada e violenta[108], é também particularmente perigoso, na medida em que se reconhece que "o recurso a uma tal técnica de investigação representa sempre o emprego de alguma deslealdade".[109] Por conseguinte, deve ser considerado um método excecional e circunscrito aos tipos de criminalidade mais grave, violenta e organizada.

Posto isto, somos invariavelmente levados a questionar se o legislador, ao ter consagrado expressamente a sua admissibilidade em crimes como o de homicídio voluntário (art. 2º/a) RJAE) e crimes contra a liberdade e autodeterminação sexual (art. 2º/b) RJAE), sem mais exigências, não terá extravasado aquilo que é entendido por criminalidade organizada, alargando, em consequência, a incidência das ações encobertas a um considerável (e desmedido) leque de crimes.[110]

Ora, o conceito de criminalidade organizada não é unânime na doutrina e varia de país para país. Porém, em Portugal, alguns autores, como Alexandre Godinho, identificam como caraterísticas essenciais da criminalidade organizada o facto de a "acção ter um carácter permanente ou [ter] alguma duração", "ter uma estrutura bem definida hierarquicamente", "busca[r] por elevados lucros monetários de forma ilegal" ou "busca[r] por um grande poder económico", assim como o facto de pressupor "a existência de um grupo composto por três ou mais pessoas."[111] Neste sentido, também o Guia Legislativo para a Aplicação da Convenção das Nações Unidas contra a Criminalidade Organizada

---

[108] Neste sentido dispõe Duarte Nunes, apontando várias razões para se crer na eficiência deste método quando em causa estão situações de criminalidade grave e violenta, entre as quais destacamos: o facto de os ataques terroristas serem imprevisíveis; o facto de estar a ela associada uma elevada capacidade e complexidade organizatória das associações criminosas; o facto de permitirem evitar a prática de novos crimes (ou minimizar as suas consequências); de tornarem mais eficazes e seguras as entregas controladas, quando as ações sejam cumuladas com aquelas; e, ainda, o facto de, nos chamados "crimes sem vítima" (e, portanto, sem denúncia) permitirem a aquisição da notícia do crime e dos respetivos elementos probatórios. *(Cf.* DUARTE ALBERTO RODRIGUES NUNES *O problema da admissibilidade… Op. Cit.*. Pg. 839).

[109] Assim o entendeu o Tribunal Constitucional no Acórdão nº 58/98 de 14 de outubro.

[110] Benjamim Silva Rodrigues considera que "esta (desmesurada e desproporcionada) ampliação do âmbito de aplicação afigura-se, sem mais, censurável, à luz do princípio da proporcionalidade e da subsidiariedade (ou preferência dos meios menos gravosos face aos mais gravosos de obtenção de prova*)." Cfr.* BENJAMIM SILVA RODRIGUES, *Da Prova Penal*: *Novos Métodos "Científicos" de Investigação Criminal nas Fronteiras das Nossas Crenças*, Tomo VI, 1ª Ed., Lisboa: Rei dos Livros, 2011. Pg. 382.

[111] *Vide:* GODINHO, Jorge Alexandra Fernandes, "*Do crime de "branqueamento de capitais": Introdução e Tipicidade*", Edições Almedina, 2001. Pg. 4 a 7.

Transnacional, no seu art. 2º-A) define "grupo criminoso organizado" como sendo "um grupo estruturado de três ou mais pessoas, existindo durante um período de tempo e actuando concertadamente com a finalidade de cometer um ou mais crimes graves ou infrações estabelecidas na presente Convenção, com a intenção de obter, direta ou indiretamente, um benefício económico ou outro benefício material".[112]

Pelas noções expostas anteriormente, podemos assim concluir que à criminalidade organizada estão associadas duas dimensões essenciais: a do tempo, no sentido de se exigir uma atividade prolongada e duradoura; e a da pluralidade de atores, na medida em que se exige a prática de atos ilícitos por, pelo menos, três pessoas. E são estas dimensões que nos levam a questionar se efetivamente a introdução, pelo legislador, daqueles tipos de crime no catálogo de crimes relativamente ao qual é permitido o recurso às ações encobertas, sem mais exigências, não foi desproporcionada.

De facto, existem dúvidas quanto a saber se os referidos crimes preenchem os requisitos necessários – de duração e de quantidade de autores - para que possa ser justificado o recurso a um tal método de investigação criminal que, como vimos, tem natureza excecional. Por outro lado, tal como elucida Sandra Pereira, mesmo relativamente ao crime de tráfico de estupefacientes (constante do art. 2º/j) RJAE), nem sempre se justificará a utilização do agente encoberto. Isto porque, estando em causa uma pequena delinquência "não se afigura proporcional e adequado", porquanto a prova de um tal ilícito sempre poderá ser feita por via de outros meios não tão gravosos e lesivos, como, por exemplo, flagrantes delitos sem intervenção de um agente encoberto.[113] Neste sentido, a autora considera, em jeito de crítica, que, tendo em conta as restrições aos direitos fundamentais que o recurso a este método de investigação acarreta, a sua utilização deveria ter sido cingida aos crimes que, de outra forma, dificilmente seriam relevados. No seu entendimento, a forma ampla como o elenco foi introduzido trouxe consigo o risco de tornar este método algo banal e generalizado.[114]

---

[112] Guia Legislativo para a Aplicação da Convenção nas Nações Unidas contra a criminalidade Organizada Transnacional. Ministério da Justiça. Vancouver, março de 2003. Disponível em https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/GuiaConv.pdf [Acesso em: 14 de jan. 2022].
[113] PEREIRA, Sandra, "*A recolha de prova…" Op. Cit.* Pg. 150.
[114] *Ibidem*. Pg. 149.

Sob outra perspetiva, o art. 2º não inclui no seu elenco outros tipos de crime cujas caraterísticas poderão ser reconduzi-los ao espetro da criminalidade grave, como é o caso dos crimes de tráfico de armas e de tráfico de obras de arte. Por outro lado, tal como denota Isabel Oneto, de igual modo se encontra excluído do catálogo o crime de administração danosa em unidade económica do sector público, que antes constava da alínea b) do nº 2 do art. 1º da Lei de Combate à Corrupção e Criminalidade Económica e Financeira.[115]

Note-se que se a incongruência, em alguns casos, ou a insuficiência, noutros, do catálogo de crimes enunciados no RJAE é percetível quando em causa está uma ação encoberta tradicional (física), tratando-se de uma ação encoberta digital essa questão impõe-se com ainda maior intensidade, o que poderá justificar o facto de o legislador ter introduzido na Lei do Cibercrime uma norma especificamente destinada a regular as ações encobertas em ambiente digital – o art. 19º da LC – em que os crimes informáticos ganham, finalmente, protagonismo. De tal forma que este último preceito possa ser lido, nas palavras de David Silva Ramalho, "como uma primeira abordagem, por parte do legislador, à autonomização das acções encobertas digitais"[116]. Assim, e ainda que de forma prematura e sujeita a algumas críticas como já evidenciámos em momento anterior[117], esta previsão legal permitiu, pelo menos, evidenciar a necessidade de revisão do âmbito de aplicação das ações encobertas.

4.2. Requisitos de admissibilidade e finalidades subjacentes às ações encobertas

A excecionalidade das ações encobertas acaba por ser densificada no art. 3º do RJAE, preceito onde o legislador procede à discriminação dos requisitos que precisam de ser cumpridos para que possam ser desencadeadas. Deste modo, o legislador começa por consagrar um princípio de adequação e proporcionalidade no recurso às ações encobertas, estabelecendo que estas devem "*adequadas aos fins de prevenção e repressão criminais identificadas em concreto*" e "*proporcionais quer àquelas finalidades quer à gravidade do crime em investigação".* Do que resulta que o recurso às ações encobertas dependerá da consideração, no caso concreto, do princípio da proporcionalidade, consagrado no art. 3º/3

[115] ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 116.
[116] DAVID SILVA RAMALHO, *Métodos ocultos…Op. Cit.* Pg. 303.
[117] *Vide:* ponto 3 da Parte II.

e reforçado no art. 18º/2 e 3 da CRP, nas suas dimensões da adequação, necessidade e proporcionalidade em sentido estrito.

De acordo com Germano Marques da Silva, aquele princípio determina que qualquer medida processual deva ter correspondência na gravidade do crime e na sanção que previsivelmente venha a ser aplicada em razão da prática do(s) crime(s) indiciado(s) no processo.[118] Significa isto que só serão admitidas as ações encobertas que, em virtude das circunstâncias do caso concreto, se mostrem adequadas, necessárias e proporcionais ao alcance dos fins que lhes estão subjacentes.[119] Tal só se configurará possível se os resultados suscetíveis de serem alcançados através dela constituírem um bem maior relativamente aos direitos, liberdades e garantias que acabam por ser colocados em causa durante a ação. Assim, nas palavras de Benjamim Rodrigues, exige-se, em concreto, que "a gravidade da intromissão (bens jurídicos ou direitos fundamentais) não [seja] desproporcionada face ao peso das razões investigatórias que «contra-motivam» ("interesses e contra-interesses") e justificam tal método".[120]

Também diretamente correlacionado com a ideia anterior está o princípio da proibição do excesso, de acordo com o qual nem todos os meios podem justificar os fins prosseguidos, só sendo sustentáveis os meios que gerem uma lesão menos gravosa do que aquela que resultaria do ataque ao bem jurídico em perigo; e, ainda, o princípio da subsidiariedade, que implica que perante a existência de uma pluralidade de métodos "abertos" e "ocultos" de investigação abstratamente aplicáveis, se dê prioridade aos "abertos" e, só no caso de esses não se revelarem aptos a satisfazer os interesses da investigação, se recorra aos métodos "ocultos", procurando sempre enveredar por aquele que se afigure como o "menos gravoso de entre aqueles que se afiguram idóneos"[121]. O que determina que sempre que os fins possam ser alcançados por outra técnica de investigação criminal menos invasiva, a autoridade judiciária competente não deva autorizar o desencadeamento de uma ação encoberta.[122]

---

[118] GEMRANO MARQUES DA SILVA, *Curso de Processo Penal… Op. Cit.* Pg. 362.
[119] *Cfr*. ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 187.
[120] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Novos Métodos "Científicos"… Op. Cit.* Pg. 70.
[121] *Cfr*. DAVID SILVA RAMALHO, *Métodos ocultos... Op. Cit.* Pg. 236.
[122] Assim, "exige-se que, em concreto, face a toda a pletora de meios de (obtenção) da prova, consagrados no CPP, nenhum deles se afigure apto, suficiente e adequado a permitir a aquisição de material probatório incriminatório". Cfr. BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Bruscamente… A(s) Face(s)*

De relevar ainda que, reproduzindo o entendimento de Susana Aires de Sousa, "a gravidade e a danosidade do crime investigado devem exigir-se relativamente a todas as infrações tipificadas no art. 2º da lei das ações encobertas: é a própria lei que pressupõe, no artigo 3º, nº1, que a ação encoberta seja proporcional à gravidade do crime que se investiga".[123] De tal forma que, já sob a ótica de Benjamim Silva Rodrigues, poderá acontecer que se esteja perante um dos crimes catalogados no art. 2º do RAJE mas que, em concreto, não adquira a gravidade suficiente para justificar a medida, sendo de evitar, nas suas palavras, "o automatismo «crime do catálogo = admissibilidade da acção encoberta» "[124]. Assim, a simples "*a simples presença de um crime do catálogo não pode, sem mais, legitimar, sem qualquer outro juízo (de proporcionalidade), a admissibilidade das acções encobertas*"[125].

Em face do exposto, tal como exemplifica Paulo Pinto de Sousa, não será justificável a infiltração de agentes, numa ação encoberta clássica, para a investigação de um simples furto de um aparelho de música numa dada residência.[126] Assim como não será de admitir, por maioria de razão, no âmbito de uma ação encoberta digital, a instalação de *malware* no computador do suspeito para a obtenção da palavra-passe do seu w*ebmail*, quando para tanto bastaria recorrer a uma injunção para concessão do acesso a dados dirigida ao fornecedor de serviços de *webmail.*[127]

Cumpre também apontar que quando nos referimos às ações encobertas como um meio de obtenção de prova de "*ultima ratio"* não falamos em termos cronológicos, mas antes em termos lógicos: por outras palavras, o seu recurso não dependerá do prévio esgotamento infrutuoso de outros meios de obtenção de prova menos lesivos, bastando, para que delas se possa lançar mão, que se conclua, no caso concreto, pela impossibilidade de se alcançar a prova desejada através de outros meios.[128]

Oculta(s) dos Métodos Ocultos de Investigação Criminal, Tomo II, 1ª Ed., Lisboa: Rei dos Livros, 2010. Pg. 125.

[123] SUSANA AIRES DE SOUSA, *Ações encobertas… Op. Cit.* Pg. 37.

[124] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Novos Métodos "Científicos"… Op. Cit.* Pg. 383.

[125] *Cfr. Ibidem* (o itálico não é nosso); Com igual posicionamento se apresenta Isabel Oneto, ao defender que "(…) ainda que adequado e necessário, o meio escolhido pode manifestar-se desproporcional à gravidade do crime em investigação." *Cfr.* ONETO, Isabel, *O Agente Infiltrado… Op. Cit*. Pg. 187 e 188.

[126] *Cfr.* PAULO PINTO DE SOUSA, *Acções Encobertas… Op. Cit.* Pg. 236.

[127] *Cfr.* DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 232.

[128] DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Cit*. Pg. 209.

Já no que respeitante às finalidades que estão subjacentes às ações encobertas dispõe o art. 3º do RJAE a possibilidade de serem prosseguidas quer finalidades de investigação preventivas, quer repressivas. Ora, esta dupla finalidade não tem tido acolhimento pacífico junto da doutrina. Costa Andrade entende ser inadmissível a utilização de "homens de confiança com propósitos e para fins unicamente repressivos, isto é, exclusivamente preordenada à repressão de crimes já consumados, em homenagem nomeadamente à ideia duma administração eficaz da justiça penal."[129] No entanto, no seu entender, o recurso a esta figura já não constituirá um meio de prova proibido (enquadrável no art. 126º/2/a) do CPP) quando a prossecução de finalidades preventivas se destine ao desmantelamento do terrorismo, da criminalidade violenta ou altamente organizada.[130] Também na mesma linha de discórdia quanto à prossecução exclusiva nas ações encobertas de finalidades repressivas se posiciona Mário Ferreira Monte, de acordo com o qual "a acção dos agentes de confiança, quer infiltrados, quer provocadores, deve ser teleologicamente fundada na prevenção e nunca [em] fins meramente repressivos"[131] , na medida em que, na sua ótica, legitimar unicamente a prossecução de finalidades repressivas seria admitir um comportamento imoral por parte do Estado. Diferentemente, Benjamim Silva Rodrigues parece não ser adepto da prossecução de finalidades preventivas, uma vez que admitir essa possibilidade seria consentir que as ações encobertas ocorressem à margem de qualquer processo criminal "em curso", o que, para si, não merece aceitação.[132]

No que respeita especificamente às finalidades subjacentes às ações encobertas que se desenvolvem em ambiente digital, a Lei não apresenta uma resposta clara. De facto, o legislador limita a investigação dos crimes a que se refere o art. 19º/1 da Lei nº 109/2009 e que não constam do art. 2º da Lei nº 101/2001 à prossecução de finalidades repressivas; já relativamente aos crimes que constam do último preceito, o legislador admite o recurso a ações encobertas (quer para fins preventivos, quer para fins repressivos), mas não identifica, de forma expressa, o tipo a que se refere: se às ações encobertas físicas - apenas e exclusivamente - ou se também às ações encobertas digitais, deixando, assim, em aberto essa possibilidade.

---

[129] MANUEL DA COSTA ANDRADE, *Sobre as proibições... Op. Cit.* Pg. 232.
[130] *Ibidem.*
[131] MÁRIO FERREIRA MONTE, *Anotação ao relatório da Comissão Europeia dos Direitos do Homem, processo nº 25829/94, Francisco Teixeira Castro contra Portugal in* Scientia Iuridica – Revista de direito comparado português e brasileiro. T. XLVI. Universidade do Minho, 1997.
[132] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Novos Métodos "Científicos"... Op. Cit.* Pg. 382.

Também diretamente correlacionada com as finalidades subjacentes às ações encobertas está a competência para a iniciativa e decisão em matéria de ações encobertas. O legislador prossegue nos números 3 e 4 do art. 2º do RAJE esclarecendo a quem compete a autorização para legitimar as ações encobertas, estabelecendo que tal varia consoante estejamos perante uma ação destinada a fazer face a finalidades preventivas ou de repressão criminal. Deste modo, estabelece-se que quando esteja em causa a prossecução de finalidades de repressão criminal, o recurso às ações encobertas, na fase de inquérito, depende de prévia autorização do magistrado do MP, não obstante essa ter de ser comunicada e validada posteriormente pelo JIC. Já no caso de a ação encoberta decorrer no âmbito da prevenção criminal, estabelece-se que a autorização para a levar a cabo deve ser requerida, antes da fase de inquérito, pelo MP ao JIC, cabendo a decisão a este último. Ora, tal ressalva afigura-se essencial, na medida em que, sendo o Juiz de Instrução aquele que, à partida, possui o maior conhecimento efetivo da causa, só ele poderá julgar da adequação e utilidade da ação encoberta ainda fora do âmbito de um processo-crime.[133] Ademais, Benjamim Silva Rodrigues, acrescenta que, atendendo à natureza da medida, não deverá esta ocorrer sem que se verifique a devida ponderação judicial ou sua ficção, sob pena de ser violado o princípio da proporcionalidade e da reserva judicial em matéria de restrição de direitos fundamentais dos cidadãos.[134]

Ora, no que tange especificamente às ações encobertas digitais, o art. 19º da Lei nº 109/2009 também se releva omisso quanto à competência para a sua iniciativa e decisão.[135] Revelando-se a competência uma matéria sensível, tendo em conta as dúvidas acrescidas que as ações encobertas em ambiente informático-digital convocam no plano jurídico-constitucional, somos levados a questionar se a regulação, de forma clara, da autorização do

[133] Assim, como elucida Benjamim Silva Rodrigues, o RAJE adota um sistema de "*validação tácita",* na medida em que, embora possa parecer, em face da redação do texto, ficar na disponibilidade do magistrado do MP a autorização para legitimar as ações encobertas, a verdade é que tal não acontecerá se, após comunicada ao *Juiz das liberdades*, este as afastar. O Autor critica este regime de "validação tácita" constante do nº 3 do art. 3º do RJAE, na medida em que considera não ser constitucionalmente admissível a restrição de direitos, liberdades e garantias sem uma prévia ponderação judicial, apontando essa possibilidade como simultaneamente incompatível com o princípio da proporcionalidade e da reserva judicial em matéria de restrição de direitos fundamentais dos cidadãos. Acrescenta ainda "a judicialização da medida [se] impõe, mais do que nunca, nos casos de prevenção criminal", uma vez que a nossa CRP apenas admite a restrição de certos direitos, liberdades e garantias, no âmbito deste tipo de investigação, quando já se tenham iniciado os respetivos processos criminais. *Cf. Ibidem.* Pg. 384.

[134] *Ibidem.*

[135] DUARTE ALBERTO RODRIGUES, *Os meios de obtenção… Op. Cit*. Pg. 224.

recurso às mesmas não deverá assumir-se como imperativa. O mesmo se diga em relação à utilização de outros meios e dispositivos informáticos no âmbito da ação, igualmente restritivos de direitos fundamentais, cuja regulação não encontra também expressão no texto da lei.[136]

4.3. O princípio da indispensabilidade probatória na anexação do relato do agente encoberto ao processo

O art. 4º do RJAE, no seu nº1, ao estabelecer que "*a autoridade judiciária só ordenará a junção ao processo do relato a que se refere o n.º 5 do artigo 3.º se a reputar absolutamente indispensável em termos probatórios*" consagra o princípio-regra da indispensabilidade probatória na anexação do relato do agente ao processo, ou seja, nele se estabelece que as provas processuais que sejam obtidas através das atividades do agente encoberto – materializados essencialmente no relato que tenha efetuado - só deverão ser consideradas e utilizadas para fundamentar a decisão do Juiz, num ou noutro sentido, se se revelarem imprescindíveis e essenciais à resolução do direito no caso concreto. Assim, a regra é, portanto, a não junção do relato do agente ao processo, o que também não tem escapado à crítica de alguma doutrina.

De acordo com Sandra Oliveira e Silva a dispensa da junção do relato ao processo só poderá acontecer quando no caso concreto se verifique uma das seguintes situações: " (1) se for previsível um grave prejuízo para a tarefa de investigação criminal, decorrente da impossibilidade da utilização daqueles agentes em ulteriores acções encobertas; (2) existir um elevado risco pessoal para o funcionário ou a sua família; (3) ou a operação oculta se tiver revelado absolutamente infrutífera do ponto de vista da recolha de provas."[137] Assim, sempre que em cause suceda uma das situações anteriores, verifica-se a possibilidade de não ser anexada ao processo a prova que tenha sido produzida no âmbito da ação encoberta. De revelar que a não anexação do relato ao processo se tem amplamente ancorado no risco para a segurança do agente que da sua anexação resultaria, tornando-se necessário salvaguardá-lo de eventuais represálias sofridas em consequência das suas atividades.

---

[136] Também neste sentido: *Ibidem.* Pg. 225.
[137] SANDRA OLIVEIRA E SILVA, *A proteção de testemunhas no processo penal*, Coimbra: Coimbra Editora, 2007. Pg. 321 (nota de pé de página 82).

Ora, embora compreendamos a opção do legislador, não podemos deixar de reconhecer que a consagração de um princípio da indispensabilidade probatória em termos absolutos poderá acarretar, na verdade, mais prejuízos do que benefícios. De facto, nem sempre a segurança do agente encoberto poderá ficar gravemente comprometida com a junção do seu relato ao processo, não sendo razoável estabelecer como regime-regra a consideração do relato apenas nos casos em que ele se revele indispensável para fazer prova dos factos. Deste modo, seria antes mais congruente a previsão de impossibilidade de junção do relato do agente ao processo apenas nos casos em que se verificasse, *in casu,* um risco sério para a sua segurança. Em todos os demais casos, em que esse risco sério não fosse uma realidade, sempre se procederia à sua junção ao processo, no respeito pelos direitos de defesa do arguido investigado.

Isto porque, tal como denota Isabel Oneto, não sendo anexado o relato do agente, os sujeitos processuais não têm efetivamente como saber a origem de determinadas imputações nem de se pronunciarem relativamente a elas[138], o que não se coaduna com as máximas do princípio do contraditório, "corolário de uma ideia de participação constitutiva dos sujeitos processuais (sobretudo o arguido) na decisão do caso"[139] e que se "materializa no direito subjectivo de intervir activamente na produção da prova",[140] especialmente quando em causa está um facto que lhe afete pessoalmente. Corrobora ainda este entendimento da premência de junção do relato ao processo o facto de a sua não junção comportar perigosos riscos ao nível da forma como a ação é conduzida, na medida em que "uma vez autorizada, na prática, a ação encoberta pode seguir rumos distintos dos autorizados".[141]

Note-se que toda esta argumentação se torna ainda mais forte e convincente quando em causa está o relato que tenha sido feito no âmbito de uma ação encoberta digital. Questionamos: fará sentido a extensão de um tal princípio a um tipo de investigação criminal que ocorre por detrás de um aparelho eletrónico, com ocultação da identidade, não se

---

[138] ISABEL ONETO, Isabel, *O Agente Infiltrado… Op. Cit*. Pg. 188 a 192. Também para esta questão alerta Costa Andrade que, em jeito de crítica ao modo como se processam os métodos ocultos de obtenção de prova, refere que a circunstância de os suspeitos investigados não terem conhecimento da medida nem antes nem durante a sua execução impossibilita-os de "*actualizar qualquer pretensão de reacção e tutela"* e de *"fazer valer a ilegalidade da medida por violação de qualquer dos pressupostos legais". Cfr.* MANUEL DA COSTA ANDRADE, *Bruscamente no verão passado… Op. Cit.* Pg. 107.

[139] SANDRA OLIVEIRA E SILVA, *A proteção… Op. Cit.* Pg. 251.

[140] *Ibidem.* Pg. 251. Também neste sentido: GERMANO MARQUES DA SILVA, *Direito Processual Penal Português… Op. Cit.* Pg. 89 e 90.

[141] SANDRA PEREIRA, *A recolha de prova… Op. Cit.* Pg. 153.

colocando, por regra, por essa razão, em questão a segurança pessoal do agente? De facto, parece-nos que a previsão de tal princípio – pelo menos com base naquele argumento -, embora possa fazer sentido (em certa medida) nas ações encobertas clássicas (físicas), se acaba por revelar desnecessária nas ações encobertas digitais em função da natureza e do próprio modo como a investigação se processa.

Por outro lado, questão de particular controvérsia – e talvez, a maior - tem sido a de saber se, anexado que seja ao processo, o relato terá ou não valor probatório por si só. Muitas têm sido as dúvidas levantadas em torno desse valor, tendo em conta a essência da prova obtida e as repercussões que a sua obtenção acabam por ter no âmago das garantias processuais do investigado.

Porém, uma análise dessa índole não poderá ser feita sem que antes compreendamos em quê que consiste afinal um tal relato e quais as finalidades que lhes estão subjacentes. Ora, o relato corresponde a um importante documento onde é descrita toda a factualidade conhecida pelo agente encoberto no exercício das suas atividades investigativas.

Dada a importância que assume, não só no sentido de permitir dar conhecimento das informações obtidas pelo agente, mas também de permitir o controlo das suas atividades, estipula o nº 6 do art. 3º do RJAE que "*a Polícia Judiciária fará o relato da intervenção do agente encoberto à autoridade judiciária competente no prazo máximo de quarenta e oito horas após o termo daquela"*. Note-se que esta exigência normativa acaba por demonstrar a forma controlada com que se pretende que as ações encobertas se desenrolem, tendo, desde logo, em conta o curto prazo que o OPC dispõe para cumprir a formalidade. Porém, a verdade é que um tal controlo não deveria estar cingido ao término da ação encoberta como a norma prevê ("*após o termo daquela").* Isto porque, a ser assim, o controlo por parte da autoridade judiciária só é efetivado em momento posterior à elaboração do relato, ou seja, nas quarentas e oito horas posteriores ao *terminus* da ação. Assim, apesar de a norma estabelecer um prazo para a apresentação do relato final feito pelo agente encoberto, não determina um marco temporal para a duração da ação encoberta, o que, na prática, determina que a mesma possa ser realizada indefinidamente e livre do necessário controlo contínuo por parte das autoridades judiciárias. Do que resulta poder ser aqui que possamos identificar, nas palavras

de Armando Dias Ramos, a "pedra de toque do RJAE" justificativa da sua inconstitucionalidade.[142]

De relevar que, como bem evidencia o autor, um tal regime tão permissivo de condutas investigativas, capaz de potenciar inúmeras violações de direitos fundamentais, não se verifica em relação a outros métodos ocultos de investigação criminal, como as interceções telefónicas, em que o legislador estabeleceu a obrigatoriedade de o OPC levar quinzenalmente ao conhecimento do MP os suportes técnicos com as interceções, assim como os respetivos autos e relatórios, posteriormente entregues ao JIC no prazo máximo de quarenta e oito horas.[143]

Compreendida que está a funcionalidade do relato do agente encoberto e as deficiências legislativas que se verificam ao nível do controlo subjacente às atividades do agente encoberto questionamos: será o relato do agente o fruto do cumprimento de uma mera formalidade legalmente imposta ou constituirá um verdadeiro meio de prova? A ser considerado um meio de prova, deverá ter valor probatório autónomo? Serão, essencialmente, sobre estas questões que nos propomos agora debruçar.

Ora, como vimos, resulta da própria Lei das Ações Encobertas a possibilidade de o agente encoberto depor em condições de anonimato, com recurso a técnicas de ocultação de imagem e/ou de distorção da voz. Por outro lado, a Lei não se mostra explícita quanto à possibilidade de o seu relato ser considerado um meio de prova, mesmo quando desacompanhado do depoimento do agente em fase de audiência de julgamento, o que tem provocado sérias controvérsias doutrinais. Em face desta última possibilidade tem-se apontado que mecanismos de uma tal índole poderão colocar em causa, desde logo, a própria ideia de dignidade dos tribunais, na justa medida em que possam converter os atos processuais em "autênticas sessões de teatro judiciário".[144] Para além disso, aponta-se ainda, de forma mais gravosa, o facto de poderem implicar uma "compressão do «direito de defesa» do arguido (art. 32º, nº1 da CRP)".[145]

Deste modo, no âmago da questão está, assim, saber até que ponto a admissibilidade de um julgamento feito naqueles moldes não chocará com um importante princípio

[142] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 69 e 70.
[143] *Ibidem.*
[144] SANDRA OLIVEIRA E SILVA, *Salas vazias e declarações anónimas. Notas sobre a proteção de testemunhas e o processo equitativo no julgamento da criminalidade organizada in* Revista do CEJ, Dossiê Temático Criminalidade Económico-Financeira e Criminalidade Organizada. 2º Semestre 2011, nº 16. Pg. 308.
[145] *Ibidem*. Pg. 308 e 309.

processual: o princípio da imediação. Um tal princípio exige precisamente que a "decisão jurisdicional só po[ssa] ser proferida por quem tenha assistido à produção das provas e à discussão da causa pela acusação e pela defesa, mas significa também que na apreciação das provas se dev[a] dar preferência aos meios de prova que se encontrem em relação mais direta com os factos probandos" [146] (os meios imediatos), pelo que se receia que a prova produzida pelo agente encoberto, muitas vezes desacompanhada do seu depoimento, possa colocar em causa estas máximas.

De facto, como evidencia Sandra Oliveira e Silva, são inegáveis as vantagens associadas ao método da imediação, entre as quais o facto de "p[ôr] a entidade decidente em contacto permanente com os chamados «factos auxiliares imponderáveis» - as informações não-verbais que irrompem na audiência de julgamento, sobretudo as que se extraem das múltiplas cambiantes do comportamento da testemunha (v.g., os gestos, o tremor, a saudação), da espontaneidade e tempestividade da narração, da constância e firmeza das respostas"[147], assim como o facto de permitir "oferece[r] a possibilidade de interrogar o declarante sobre o conteúdo preciso do seu testemunho, de modo a colmatar lacunas ou esclarecer contradições, e sobre outros aspectos relevantes, objectivos ou subjectivos, do prisma da credibilidade do depoimento".[148]

É em face daquelas vantagens, garantidoras de um processo penal mais justo e transparente, que Paulo Pinto de Albuquerque defende que o relato desacompanhado do depoimento não tem qualquer força probatória na audiência de julgamento, em respeito ao princípio da imediação. Entende o autor que só o depoimento pessoal do agente poderá valer como "meio de prova do que ele fez, viu e ouviu", não creditando valor autónomo ao relato por si só. No seu entendimento, "o relato serve essencialmente um outro propósito, que não a documentação da prova: ele serve para que a autoridade judiciária possa controlar a contínua "adequação" da acção encoberta e decidir sobre a sua prorrogação, modificação e cessação." [149]

---

[146] GERMANO MARQUES DA SILVA, *Direito Processual Penal Português… Op. Cit.* Pg. 104.
[147] SANDRA OLIVEIRA E SILVA, *A proteção… Op. Cit.* Pg. 236
[148] *Ibidem.* Pg. 236 e 237.
[149] PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, 4.ª edição atualizada, Lisboa: Universidade Católica Editora, 2018. Pg. 685; Em sentido semelhante se posicionou já o STJ, afirmando expressamente que "o relato em si, enquanto documento descritor daquilo a que o agente assistiu, não tem valor probatório" *Vide*: Acórdão do STJ de 10 de março de 2016. Disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/f0734c070225ad5e80257f78003f16cd?OpenDocument [Acesso em: 12 de março de 2022].

Duarte Nunes vai ainda mais longe, defendendo que mesmo que o relato seja acompanhado do depoimento do agente, o recurso à ocultação da sua identidade em sede de audiência de julgamento representa um atentado para os direitos da defesa e para o princípio da imediação ("(…) pois o Juiz não consegue visionar a reação e/ou a postura da testemunha quando lhe são colocadas as questões e enquanto responde às mesmas, aspetos que poderão ser importantes para aferir a credibilidade do seu depoimento)"[150]. Do que resulta que, para o autor, o relato só possa corresponder a um mero elemento de controlo da legalidade que não tem valor probatório por si só.[151]

Já no polo oposto, autores como Nivaldo Filho, consideram antes que a prova que resulte da atuação do agente encoberto – corporizada tanto no relato como no seu depoimento – deverá ter um valor probatório por si só (autónomo), uma vez que, se assim não fosse, estaríamos a descredibilizar a atividade do agente encoberto, legitimada no nosso ordenamento jurídico. De acordo com o autor, estando as ações encobertas expressamente reguladas em diploma próprio, sujeitas à observância de requisitos específicos e à decisão de uma autoridade judiciária, o relatório, mesmo desacompanhado do depoimento do agente, deverá continuar a revestir-se de qualidade probatória.[152]

Ora, entre nós, não desprovendo de sentido qualquer uma das teses anteriores, optamos por nos colocar numa posição intermédia. Acompanhamos, assim, de perto o pensamento de Sandra Pereira que, em jeito de questionamento, acaba por resumir o nosso entendimento: "Qual o sentido de não atribuir qualquer valor probatório ao relato quando ele só foi junto ao processo por ser indispensável em termos probatórios? Mas, por outro lado, admitir que o relato do agente infiltrado sobre a ação encoberta te[nha] algum valor probatório [não será] amputar em grande medida o sentido útil do princípio da imediação [?]".[153] Assim, socorrendo-nos das palavras de Isabel Oneto, entendemos que o relato aqui em análise não poderá ser visto como a "observação de uma mera formalidade, mas uma peça processual crucial"[154]. Nesse sentido, o relato constitui um crucial e verdadeiro meio de prova, na medida em que é nele que estão registados, de forma perpétua, os pormenores

[150] DUARTE ALBERTO RODRIGUES NUNES, *O Problema da Admissibilidade… Op. Cit*. Pg. 883.
[151] *Ibidem.* Pg. 889.
[152] NIVALDO MACHADO FILHO, *O Agente Infiltrado em duelo com o contraditório: aspectos críticos de seu relatório e depoimento* in Revista de Concorrência e Regulação, Ano VIII. Número 31, julho/setembro de 2017. Pg. 113.
[153] SANDRA PEREIRA, *A recolha de prova … Op. Cit.* Pg. 153 e 154.
[154] OISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 188 e 189.

subjacentes à ação encoberta, capazes de corroborar o depoimento do agente bem como de apoiar o Juiz na tomada de decisão mediante a posse de documento escrito dotado de qualidade probatória. Trata-se, na verdade, de um documento que permite não só o controlo judicial da ação encoberta, como também o registo de importantes aspetos atinentes à mesma (relativos, por exemplo, à forma como foi desencadeada e concretizada, à autoria e aos factos em apuração), que poderão servir de prova tanto à acusação como à defesa.

No entanto, não podemos deixar de reconhecer que é um meio de prova que acaba por suscitar dúvidas, na medida em que advém de um método de investigação que é, ele próprio, reticente. Deste modo, apesar de as ações encobertas beneficiarem de um regulamento próprio, de estarem sujeitas à observância de requisitos específicos e à decisão de uma autoridade judiciária, a verdade é que acarretam inevitavelmente a restrição de direitos, liberdades e garantias dos cidadãos-alvo e, em geral, de importantes princípios processuais. Assim sendo, como forma de se obviar este último aspeto entendemos que seria fundamental a anexação do relato do agente encoberto ao processo, em derrogação do princípio da indispensabilidade probatória previsto no art. 4º/1 do RJAE (salvo em circunstâncias devidamente justificadas). Anexado que fosse o relato, seria ainda essencial o depoimento do agente encoberto, uma vez que só esse permite melhor efetivar as regras e princípios que presidem ao processo penal, ao mesmo tempo que permite conferir ao relato uma maior força probatória. De revelar que seria igualmente vantajosa a apresentação, pelo agente, de outros meios de prova corroborantes da prova produzida, como fotografias, vídeos e/ou áudios, capazes de melhor sustentar a tese e a prova exibida, sobretudo quando preste depoimento com ocultação da sua identidade. Na verdade, qualquer agente que se preste a "um bom serviço" procurará naturalmente por recolher o maior número de provas possível, até por uma questão de mérito profissional. Do que resulta que, nas palavras de Vitor Paiva, "a fonte autónoma de comprovação do relato ou do depoimento do agente encoberto poderá ser – e será, quase sempre – qualquer uma permitida por lei (uma busca, uma apreensão, uma escuta, por exemplo). E o meio de prova corroborante poderá ser documental, pericial, material."[155]

Em face do exposto, subscrevemos inteiramente a posição de Sandra Pereira, de acordo com a qual "o relato (…) terá de implicar necessariamente o chamamento do agente

[155] VITOR PAIVA, *Agente infiltrado, no âmbito de ação encoberta, in* Revista do Ministério Público. ISSN 0870-6107. A. 35, nº 137, 2014. Pg. 210 e 211.

infiltrado a depor em audiência de julgamento e deverá ser corroborado por outros meios de prova. Nessa medida, o relato não terá valor probatório por si só, mas tê-lo-á em conjugação com os demais meios de prova. Só desta forma é que se poderá dar coerência ao regime sem ignorar a letra da lei".[156] No entanto, concordamos com Nivaldo Filho na parte em que dispõe que a comparência do agente em audiência permitirá robustecer o conteúdo do seu relato[157], sem que isso implique a aniquilação do seu valor probatório.

Já no que respeita ao depoimento em si mesmo, obviamente que, na nossa ótica, o depoimento direto terá um valor probatório bem mais satisfatório do que o depoimento que seja feito pelo agente com recurso a técnicas que ocultem a sua identidade, dado que o primeiro responde de forma mais eficiente ao princípio do contraditório e da imediação processual. De facto, como defende Sandra Pereira, já mencionada por nós, "o depoimento do agente infiltrado em condições de anonimato levanta problemas porque colide com princípio estruturais do processo penal"[158], na medida em que não permite um contacto direto e imediato dos sujeitos processuais com a testemunha anónima, nem a possibilidade de a contra-interrogar de forma plena e efetiva.[159]

De relevar ainda que sempre que o agente deponha com ocultação da identidade, atuando, no fundo, como uma testemunha anónima, a Lei aponta no sentido de o seu relato ter de ser corroborado por outros meios de prova. Assim, a Lei de Proteção de Testemunhas nº 93/99, prevê no nº1 do seu art. 19º que "a testemunha a quem for concedida a medida de não revelação de identidade pode prestar depoimento ou declarações com recurso à ocultação de imagem ou à distorção da voz ou à teleconferência", porém, acrescenta, no número seguinte, que "nenhuma decisão condenatória poderá fundar-se, exclusivamente, ou de modo decisivo, no depoimento ou nas declarações produzidas por uma ou mais testemunhas cuja identidade não foi revelada." Significa isto que é a própria Lei que

---

[156] SANDRA PEREIRA, *A recolha de prova… Op. Cit.* Pg. 154.
[157] NIVALDO MACHADO FILHO, *O Agente Infiltrado… Op. Cit.* Pg. 113.
[158] SANDRA PEREIRA, *A recolha de prova… Op. Cit.* Pg. 156.
[159] Note-se que não contestamos, em determinados casos, a necessidade de se recorrer a métodos de ocultação da identidade do agente no momento do seu depoimento por variadíssimas razões, entre as quais destacamos o facto de a revelação poder ter como consequência a impossibilidade de o agente poder voltar a atuar nessa condição em casos futuros (o que, numa perspetiva de rentabilização de recursos, não será eficiente, dado não haver certamente muitos agentes ou terceiros especialmente preparados e treinados para assumir essas funções junto dos Departamentos de Polícia); e, sobretudo, mais importante, o facto de a sua revelação poder ter como consequência máxima indesejável a colocação do agente em risco sério de vida, assim como dos seus familiares e/ou amigos mais próximos. Porém, a verdade é que nem sempre estes perigos constituem uma realidade.

estabelece expressamente que, nestes casos, o depoimento do agente não bastará para a condenação do arguido: "tais declarações deverão ser corroboradas em medida determinante por elementos provenientes de fontes probatórias distintas que permitam concluir pela sua veracidade."[160]

Note-se que concorrem para um tal regime inúmeras razões justificativas entre as quais destacamos a "menor fiabilidade das declarações de testemunhas anónimas"[161] e as "dificuldades objectivas do arguido e do próprio julgador na fiscalização daquele material probatório."[162] Tal como sublinha Sandra Oliveira e Silva, um tal regime, derrogador do princípio da livre apreciação da prova, deverá valer mesmo nos casos em que o Juiz esteja seguro da veracidade do conteúdo do meio de prova. Nas suas palavras "neste domínio, para sustentar a condenação, a «certeza moral» do julgador tem que combinar-se com a «certeza legal» ".[163]

Sucede que a exigência de corroboração com outros meios de prova só está prevista para as decisões de condenação, já não valendo para as decisões de absolvição, caso em que preside antes o princípio da livre convicção do tribunal na apreciação do valor da prova.[164] Em face disto, Sandra Oliveira e Silva alerta, em jeito de crítica, que o legislador, apenas preocupado com os riscos de uma condenação injusta, assente num material probatório particularmente duvidoso, porque adquirido com desvios ao contraditório, não estendeu a exigência de corroboração às declarações de conteúdo favorável ao arguido, esquecendo a possibilidade de uma decisão absolutória também poderem resultar injustiças. [165]

Assim, não obstante os inúmeros problemas que possam ser convocados e independentemente da posição que se adote relativamente à centralidade que assumam (ou não) no processo, só podemos considerar, na esteira de Nivaldo Filho, que tanto o relato como o depoimento do agente encoberto, configuram dois valiosos meios de prova, uma vez que advêm da pessoa mais habilitada para prestar esclarecimentos e informações sobre os factos em juízo, tendo em conta que neles participou e deles conheceu importantes detalhes

[160] SANDRA OLIVEIRA E SILVA, *A proteção… Op. Cit.* Pg. 295.
[161] *Ibidem*. Pg. 322 e 323.
[162] *Ibidem.* Pg. 323.
[163] *Ibidem*. Pg. 323.
[164] SANDRA PEREIRA, *A recolha de prova… Op. Cit*. Pg. 158.
[165] SANDRA OLIVEIRA E SILVA, *A proteção… Op. Cit.* Pg. 318.

de planeamento e execução. São, em suma, "portadores potenciais de valiosas informações para o deslinde dos factos criminosos em apuração".[166]

4.4. A previsão da atribuição de uma identidade fictícia

No art. 5º do RJAE, o legislador, numa contínua "manifestação formal e material da preocupação de segurança exigível quanto ao agente encoberto"[167], estabelece que o último pode exercer as suas atividades de investigação e, posteriormente, o seu testemunho ao abrigo de uma identidade fictícia, atribuída por despacho do Ministro da Justiça, mediante proposta do diretor nacional da Polícia Judiciária.[168] Essa prerrogativa é válida por um período de seis meses prorrogáveis por períodos de igual duração, devendo o despacho que a atribui ser secreto e incluir a referência à verdadeira identidade do agente. Dadas as suas especificidades, esse despacho constitui um documento que integra o chamado Segredo de Estado, estando por isso também sujeito ao Regime do Segredo de Estado, regulado na Lei Orgânica nº2/2014 de 6 de agosto.

Por outro lado, tem sido ainda de entendimento pacífico que, sendo posteriormente chamado a prestar depoimento daquilo que "viu e ouviu" em sede de audiência de julgamento, o agente possa figurar como se de uma testemunha se tratasse, beneficiando das regras previstas na Lei de Proteção das Testemunhas – Lei nº 93/99, especialmente as relativas à ocultação da imagem e distorção da voz, ínsitas nos artigos 4º e seguintes da mesma Lei, e desde que cumpridos os requisitos cumulativos enunciados no art. 16º do Diploma.

Feitas estas considerações, cumpre agora aferir o sentido material do preceito. Ora, se o art. 5º do RJAE preserva toda a sua utilidade e conveniência quando em causa está a atuação do agente encoberto físico, o mesmo não poderemos afirmar quando em questão estão as atividades investigativas de um agente encoberto em espaço digital. De facto, tomando por base a *ratio legis* da norma que vimos já estar diretamente relacionada com a necessidade de assegurar a segurança pessoal do agente (e seus familiares ou entes mais

[166] NIVALDO MACHADO FILHO, *O Agente Infiltrado… Op. Cit.*. Pg. 133
[167] FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE, *O novo regime jurídico do agente infiltrado, comentado e anotado – legislação complementar,* Coimbra: Livraria Almedina. 2001. Pg. 102.
[168] Isabel Oneto nota, porém, que a atribuição de uma identidade fictícia está reservada a agentes da polícia criminal, não sendo extensível a terceiros que atuem sob o controlo da PJ. *Cfr.* ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 117.

próximos), questionamos se fará sentido a previsão de atribuição de uma identidade fictícia - pelo menos nos moldes em que está legalmente prevista - a uma figura que atua já, de princípio, por detrás de um aparelho eletrónico, de forma totalmente virtual e oculta.

Ademais, da norma não resulta claro o que se possa entender por "identidade fictícia", sendo igualmente legítimo questionar se o mero facto de o agente utilizar nas suas atividades, em espaços virtuais como c*hats* ou *blogs,* um nome fictício (o chamado *"username" ou "nickname")* equivalerá à utilização de uma autêntica identidade fictícia.

Por fim, a Lei também não faz qualquer referência a eventuais limites à criação de identidades fictícias virtuais, o que pode abrir espaço a situações de abuso na produção de prova no âmbito de ações encobertas digitais.

4.5. A isenção de responsabilidade criminal do agente encoberto

O art. 6º do RJAE, último artigo que merece a nossa consideração, trata da isenção de responsabilidade do agente encoberto. Nele se estabelece que "*não é punível a conduta do agente encoberto que, no âmbito de uma acção encoberta, consubstancie a prática de actos preparatórios ou de execução de uma infracção em qualquer forma de comparticipação diversa da instigação e da autoria mediata, sempre que guarde a devida proporcionalidade com a finalidade da mesma."*

Deste modo, prevê a norma a possibilidade de o agente encoberto poder ser desresponsabilizado penalmente pela prática de qualquer ato reputado de ilícito, desde que, em concreto, não se releve instigador, isto é, em consonância com o art. 26º, *parte final,* do CP, não determine dolosamente outra pessoa à prática do facto e haja execução ou começo de execução. De relevar que, como explica Figueiredo Dias, instigador apenas será "unicamente quem produz ou cria de forma cabal (…) no executor a decisão de atentar contra um certo bem jurídico-penal através da comissão de um concreto ilícito típico; se necessário inculcando-lhe a ideia, revelando-lhe a sua possibilidade, as suas vantagens ou o seu interesse, ou aproveitando a sua plena disponibilidade e acompanhando de perto e ao pormenor a tomada de decisão definitiva pelo executor"[169]. Do que resulta, assim, que o instigador detenha não só o domínio da vontade, como também o domínio da decisão do instigado, verdadeiramente capaz de o determinar à prática do crime. Nesses casos, embora

[169] JORGE DE FIGUEIREDO DIAS, Direito *Penal: Parte Geral, Tomo I: Questões Fundamentais, A Doutrina Geral do Crime,* 3ª Edição, Coimbra: Gestlegal, 2020. Pg. 932.

o ilícito seja obra pessoal do "homem-da-frente" (o instigado), a verdade é que a sua atuação, executada voluntariamente, é o fruto de uma decisão previamente criada ou produzida no seu espírito pelo "homem-de-trás" (o instigador).[170]

Por outro lado, determina ainda o preceito a punibilidade do agente encoberto como autor sempre que este atue como agente mediato do crime, isto é, execute o facto por intermédio de outrem (*cfr.* art. 26º, *2ª parte,* do CP). Tal sucederá sempre que o "homem-de-trás" (aquele por "cuja autoria se pergunta") possua sobre o "homem-da-frente" (o executor, intermediário ou "instrumento") o domínio da vontade, isto é, "quando o homem-de-trás coage o homem-da-frente à prática da ação (domínio da vontade por coação) ou quando o engana e o torna assim em executor involuntário do seu plano delituoso (domínio da vontade por erro)."[171]

Deste modo, pretendeu o legislador, ao estatuir um preceito nestes moldes, repudiar qualquer atividade investigativa reconduzível à figura do agente provocador, método proibido de prova entre nós, cuja expressão processual se manifesta no art. 126º/2/a) do CPP. Efetivamente, "um Estado de Direito democrático, dotado de um processo penal de estrutura acusatória temperado pelo princípio da investigação, teria inerentemente de defender e impor aos operadores judiciários a obrigatoriedade de actuarem legal e eticamente"[172], não podendo ser permitida uma investigação cujos resultados fossem obtidos a qualquer custo[173], nem podendo os agentes se valer de uma desresponsabilização ilimitada na prática de atos investigatórios. De maneira que a exclusão da sua responsabilidade dependerá da verificação, no caso concreto, do modo específico como o agente conseguiu obter a prova desejada, sendo certo que, acompanhando o pensamento de Duarte Rodrigues Nunes, o agente encoberto não tem de ser completamente passivo na sua atuação, podendo, por

[170] *Cfr. Ibidem.*
[171] *Ibidem*. Pg. 906.
[172] FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE, *Lei e Crime: O agente infiltrado versus o agente provocador… Op. Cit.* Pg. 144 e 145.
[173] Nas palavras de Germano Marques da Silva, "a eficácia da Justiça é também um valor que deve ser perseguido, mas, porque, numa sociedade livre e democrática os fins nunca justificam os meios, só será louvável quando alcançada pelo engenho e arte, nunca pela força bruta, pelo artifício ou mentira, que degradam quem as sofra, mas não menos quem as usa". *Cfr.* GERMANO MARQUES DA SILVA, *Direito Processual Penal Português… Op. Cit.* Pg. 81.

exemplo, colocar, de forma natural e sem sujeitar o investigado a qualquer forma de pressão psicológica, questões cuja resposta possam vir a ser utilizadas como prova incriminatória.[174]

A título de exemplo, tal como entendeu o STJ, no Acórdão de 14 de maio de 1997[175], não podemos atribuir responsabilidade criminal, nem considerar como provocador, o agente da PSP que tenha perguntado ao arguido se tinha droga para lhe vender, ao que lhe foi respondido que naquele momento não tinha, mas que iria a casa buscar quatro embalagens de heroína para proceder à venda. Isto porque, em casos desta índole, se entende que o agente não levou o arguido à prática do crime, nem se configurou estar em causa método de obtenção de prova proibido pelo art. 126º do CPP. Na verdade, o arguido já detinha ilicitamente droga na sua posse num momento anterior à conversação iniciada pelo agente, pelo que a questão da (ir)responsabilidade deste último nem se coloca. Coisa diferente sucederá quando um agente da PSP determine o suspeito à prática do crime, insistindo várias vezes para que ele obtenha a droga a fim de lhe a vender, induzindo-o e instigando-o à prática de um crime que, de outra forma, não teria sido praticado, como sucedeu no caso sobre o qual se debruçou o STJ no Acórdão de 15 de janeiro de 1997, bem como no Caso Teixeira de Castro c. Portugal vertido no Acórdão do TEDH de 9 de junho de 1998.[176] Do mesmo modo, por maioria de razão, em contexto informático-digital, a criação, pelo agente, de *hiperlinks* que permitam dar acesso a conteúdo pedopornográfico e cujo objetivo resida apenas em dar conhecimento aos OPC do endereço de IP da ligação a partir da qual se iniciou a comunicação de um suspeito já integrado naquelas redes ilícitas deverá ser sujeita a um igual juízo de isenção de responsabilidade.[177]

Em face do exposto, e embora esta isenção de responsabilidade seja alvo de inúmeras controvérsias doutrinais, entendemos que o agente – físico ou digital - pode prestar atividade informativa do crime, mas não pode com ela se tornar provocador e/ou responsável por um crime que, muito provavelmente, de outra forma não teria sido praticado. Do que

---

[174] DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Cit*. Pg. 215; Também neste sentido se posiciona Isabel Oneto, de acordo com a qual "o agente infiltrado é mais do que um simples observador, é um participante activo na actividade criminosa. Insere-se no mundo do crime, convive com os criminosos, ganha a sua confiança e comete crimes, quer na forma de cumplicidade, quer como co-autor ou mesmo como simples autor. Apenas lhe está vedado agir como instigador e como autor mediato". *Cfr*. ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 137.

[175] Exemplo retirado da obra FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE*, O novo regime… Op. Cit.* Pg. 103.

[176] *Cfr.* FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE, *Lei e Crime: O agente infiltrado versus o agente provocador… Op. Cit.* Pg. 266 e 267.

[177] DAVID SILVA RAMALHO, *A investigação criminal na Dark Web in* Revista da Concorrência & Regulação, ano IV, nº 14/15 (abril/setembro), 2013. Pg. 417 e 418.

resulta o agente poder, dentro dos limites impostos pelo princípio da proporcionalidade, praticar todos os atos que repute necessários para alcançar a verdade dos factos.

Porém, não podemos engar que a questão da (ir)responsabilidade criminal do agente por factos ilícitos que tenha praticado não se reveste de simplicidade. De facto, é relativamente frequente o agente encoberto levar a cabo práticas que possam com alta probabilidade vir a aliciar e a persuadir o investigado à prática do crime (podendo, inclusivamente, criar nele essa vontade sem que existisse antes uma qualquer intenção criminosa). Nesses casos é válido interrogar se o agente não deverá ser responsabilizado criminalmente por se apresentar como um verdadeiro instigador/ provocador, não obstante atue com o mero objetivo de fazer prova da prática de crimes.

Ora, segundo Sousa Aires de Sousa, alguma parte da doutrina – inserível na teoria clássica - tem defendido que a isenção de responsabilidade do agente encoberto dever-se-á fundar na "falta d[o] duplo dolo exigido na instigação, uma vez que o agente, embora tendo dolo de determinar, convencer, de criar a intenção criminal, não tem dolo de consumação do crime"[178]; já outros autores – inserindo-se na chamada teoria da tentativa impossível – consideram que a desresponsabilização se funda no facto de a "intenção criminal do provocador nunca passar de uma tentativa inidónea ou impossível, uma vez que o resultado jamais será realizado".[179] O mesmo será dizer que a isenção de responsabilidade se deve ao facto de se estar perante uma tentativa "levada a cabo com meios inaptos ou sobre objeto essencial inexistente"[180], isto é, uma instigação à qual sucede a prática de um facto criminoso não consumado por manifesta inaptidão dos meios ou carência do seu objeto.

Sob outra perspetiva, é ainda de relevar que deverá ser sujeita a um juízo diferente a situação em que os agentes encobertos, para poderem aceder a uma determinada organização criminosa, tenham que, como prova de fidelidade, praticar determinados atos ilícitos, em autoria material singular. Nestes casos, somos levados a afastar a responsabilidade do agente, na medida em que a prática desses mesmos crimes se funda em

[178] SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit.* Pg. 1226; No que a este "duplo dolo" respeita, entende Figueiredo Dias que deve, por um lado, referir-se à determinação do instigado e, por outro, ao facto por este cometido, ao menos em início de execução. Ora, pertencendo este segundo aspeto do dolo – a determinação de outrem a um concreto facto punível - à essência da instigação, ao dolo do instigador pertencerá também a representação dos concretos elementos e circunstâncias do ilícito-típico respetivo. *Cfr*. JORGE DE FIGUEIREDO DIAS, *Direito Penal: Parte Geral, Tomo I... Op. Cit.* Pg. 945.
[179] SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit.* Pg. 1227
[180] JORGE DE FIGUEIREDO DIAS, *Direito Penal: Parte Geral, Tomo I... Op. Cit*. Pg. 835.

razões ponderosas: por um lado, o *animus* do agente é investigativo, por outro lado, a intenção é proteger o bem jurídico tutelado pelos tipos penais e não ofendê-los (inexistindo, assim, qualquer dolo), atuando o agente no estrito cumprimento de um dever legal, capaz de excluir a própria tipicidade e ilicitude da conduta.[181] De relevar que estaremos perante situações em que não haveria, pois, outra forma de o agente se infiltrar e não levantar suspeitas quanto à sua identidade. Do que resulta que, nas palavras de Isabel Oneto, "considerar que (…) estaríamos perante uma provocação ao crime seria tornar inoperantes as ações encobertas, nomeadamente quando visam atingir níveis operativos superiores da associação criminosa em que se insere".[182]

Note-se que esta isenção de responsabilidade do agente afigura-se-nos ainda mais premente e complexa quando em causa está uma investigação em ambiente informático-digital. Efetivamente, se o preceito em questão já levantava dúvidas nas investigações efetuadas no plano físico, maiores problemas suscita quando em causa está a atuação do agente encoberto digital, atendendo às caraterísticas que o próprio ambiente digital apresenta e à forma inevitavelmente mais comprometida com que o agente necessita de se envolver no meio criminoso para nele poder aceder.

Finalmente, questão de particular relevância e para a qual também não conseguimos encontrar resposta no texto da lei é o que sucederá à prova que tenha sido obtida pelo agente que tenha atuado ilicitamente, isto é, fora dos limites previstos no art. 6º do RJAE. Também neste sentido parece interrogar Susana Aires de Sousa, ao questionar se deverá haver um "contínuo entre a ilicitude penal e a ilicitude processual penal".[183] Fernando Gonçalves, Manuel Alves, João Valente e Manuel Monteiro Guedes, apoiando-se na decisão do TC vertida no Acórdão nº 578/98, entendem que sendo a atividade do agente provocador ilícita

---

[181] Também neste sentido: MARINA STANGHERLIN, FABIANO AUGUSTO PETEAN, *Agente Infiltrado – Sua natureza jurídica na produção digital de provas,* 1ª Edição, Editora Appris, ISBN: 978-65-250-0902-5, 2021. Pg. 56 e 57; MANUEL AUGUSTO ALVES MEIREIS, *O Regime… Op. Cit.* Pg. 164; FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE, *Lei e Crime – O Agente Infiltrado Versus o Agente Provocador – Os Princípios do Processo Penal,* Coimbra, 2001. Pg. 267 e 268; FERNANDO GONÇALVES, MANUEL MONTEIRO GUEDES VALENTE, JOÃO MANUEL ALVES, *O novo regime … Op. Cit*. Pg. 44.

[182] ISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 149

[183] SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit.* Pg. 1235; Isabel Oneto coloca a mesma questão para o caso em que inexista autorização para a realização da ação encoberta, apontando que a resposta à mesma dependerá da posição que se adote quanto à tese da inadmissibilidade generalizada dos meios de prova que corporizem um ilícito material substantivo. *Cfr*. ISABEL ONETO, *O Agente Infiltrado… Op. Cit.* Pg. 196.

as provas obtidas não poderão deixar de ser consideradas também elas ilícitas e proibidas, por inadmissíveis, face, desde logo, ao art. 125º do CPP, que estabelece expressamente que apenas «*são admissíveis as provas que não forem proibidas por lei*»[184].

No entanto, acompanhando o pensamento da autora *supra* citada, o legislador deveria ter sido mais cuidadoso na regulamentação deste ponto, uma vez que "se considerarmos que há uma autonomia entre os dois mundos e que as categorias da ilicitude substantiva não têm lugar no domínio processual, a circunstância de o comportamento que determina o material probatório ser penalmente ilícito (havendo instigação ou autoria mediata) não terá relevo no processo penal, logo não determina a invalidade das provas obtidas mediante provocação".[185]

5. Conclusões preliminares

Chegados aqui, torna-se possível tecer as primeiras considerações sobre a legislação processual penal que se debruça sobre a figura do agente encoberto digital.

A análise que fizemos permitiu-nos compreender que a legislação processual portuguesa em matéria de cibercriminalidade continua a ser, de forma preocupante, o resultado da transposição de diretivas, decisões-quadro e outros diplomas oriundos das instâncias europeias, em atos isolados e dispersos. Por consequência, essa dispersão legislativa, agravada pela aplicação de um regime geral previsto em lei extravagante, coloca sérios problemas na regulação das questões de cibercriminalidade e, em concreto, do agente encoberto digital.

Embora seja já notória a preocupação e avanço no sentido da autonomização da figura de que nos ocupamos, a verdade é que é ainda tendência global a não distinção clara entre as ações encobertas físicas e as digitais. De facto, existe uma certa perceção de que a escassez legislativa no que respeita às atividades do agente encoberto digital poderá ser compensada pela aplicação direta, por remissão ou analogia, do regime que está previsto

[184] FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE, *Lei e Crime: O agente infiltrado versus o agente provocador… Op. Cit.* Pg. 261; Também neste sentido: GERMANO MARQUES DA SILVA, *Bufos, infiltrados e arrependidos. Os princípios Democrático e da Lealdade em processo penal in* Direito e Justiça, Revista da Faculdade de Direito da Universidade Católica, Vol. VIII, II, 1994. Pg. 29; *Idem*, *Curso de Processo Penal… Op. Cit.* Pg. 173 e ss.
[185] SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit*. Pg. 1235.

para as investigações em ambiente físico.[186] Porém, o direcionamento da figura do agente encoberto informático-digital ao substrato jurídico do agente físico revela-se redutor.

Assim, como avança Pellucci, a solução de aplicação por analogia e remissão deveria ser complementar e não substitutiva, tendo em conta que só a regulamentação autónoma deste inovador método oculto de investigação criminal permitiria diferenciar o espaço digital e conferir maior segurança ao trabalho investigativo nesse meio. Como bem elucida o autor, não podemos deixar de ter em conta que na atual sociedade informatizada, cada vez mais as informações que poderão estar constituir a base da prova processual deixam de estar guardadas em documentos "palpáveis", para passar a constar de servidores situados a quilómetros de distância ou em *bytes* armazenados em pequenos cartões de memória, pelo que deverá ser empregue um maior esforço na resposta a uma criminalidade que se assume cada vez mais tecnológica.[187]

Ora, a equiparação legal das realidades inerentes às ações encobertas físicas e digitais acaba por se revelar desadequada, na medida em que, no nosso concreto ordenamento jurídico, nem o RJAE nem a LC não se mostram capazes de responder eficientemente a todos os problemas que as últimas convocam.

Da análise do art. 19º da LC, observámos que, embora a intenção legislativa que lhe tenha estado subjacente possa ter sido profícua, a verdade é que o preceito limita-se a ampliar a investigação oculta em ambiente digital a um leque muito vasto de crimes, abrindo espaço ao desencadeamento de investigações desta índole no âmbito de ilícitos para os quais estão previstas penas relativamente baixas e com gravidade mediana. Por outro lado, é igualmente detetável uma certa discrepância entre si e o art. 2º do RJAE ao nível da amplitude do catálogo de crimes.

Ademais, para além de a norma se limitar a ampliar o catálogo ínsito naquele art. 2º do RJAE, sem nele obter correspondência, continua a nada prever quanto aos específicos e concretos meios e dispositivos informáticos passíveis de serem utilizados no âmbito de uma ação encoberta digital.

De facto, também no nº 2 do art. 19º da LC se observa a mera remissão da regulação das ações encobertas digitais para outros métodos de investigação já com um espaço próprio de regulamentação no CPP, ínsito nos artigos 187º a 189º daquele Diploma, não se

[186] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 248.
[187] *Ibidem*. Pg. 248.

especificando o que se entende por "*recurso a meios e dispositivos informáticos*", nem em que medida se poderá operar. A LC parece considerar bastante na regulamentação da utilização de tais "meios e dispositivos informáticos" as regras que estão previstas para a interceção de comunicações, o que poderá convocar algumas insuficiências. Isto porque, atenta a definição de interceção, constante do art. 2º/e) da Proposta de Lei nº 289/X/4 – LC, e a noção de agente encoberto, patente no art. 1º/2 do RJAE (para o qual remete o art. 19º da LC aqui em análise), somos levados a considerar que a remissão da ação encoberta a uma mera interceção de comunicações se poderá revelar excessivamente simplista, com a equiparação e redução a "um único mundo" de dois modos de investigação que são completamente distintos entre si.

Já no que respeita à Lei nº 101/2001 de 25 de agosto, que também mereceu a nossa melhor consideração, não conseguimos encontrar resposta na definição de ação encoberta avançada no seu art. 1º, nº 2, relativamente ao modo e condições em que o agente encoberto digital poderá atuar caso seja um terceiro. Por outro lado, também o catálogo de crimes ínsito no RAJE se, por um lado, se revela demasiado permissivo e amplo, "abrindo portas" à ação encoberta a um vasto tipo de crimes, por outro, acaba por deixar de fora outro tipo de criminalidade em que este método de investigação poderá assumir-se pertinente.

Ainda sob outro enfoque, no que respeita especificamente às finalidades subjacentes às ações encobertas que se desenvolvem em ambiente digital, observámos que a investigação nos crimes a que se refere o art. 19º/1 da Lei nº 109/2009 e que não constam do art. 2º da Lei nº 101/2001 está reservada à prossecução de finalidades repressivas; já no que respeita aos crimes que constam do referido art. 2º do RAJE, o legislador não é claro, na medida em que admite o recurso a ações encobertas (quer para fins preventivos, quer para fins repressivos), mas não identifica o tipo a que se refere: se às ações encobertas físicas (apenas e exclusivamente) ou se também às ações encobertas digitais. Ademais, também inexiste qualquer especificação no respeitante à regulação da competência para a iniciativa e decisão das ações encobertas digitais, revelando-se, uma vez mais, o art. 19º da LC, omisso nessa matéria. E o mesmo se diga em relação à utilização de outros meios e dispositivos informáticos no âmbito da ação.

Um outro problema que identificámos prende-se com o art. 4º do RJAE. O preceito, analogicamente aplicado às ações encobertas digitais, ao consagrar o princípio-regra da junção do relato do agente apenas nos casos de indispensabilidade probatória, ancorada

fundamentalmente no argumento da necessidade da proteção da segurança do investigador, perde completamente, no âmbito informático-digital, o seu sentido, em face das caraterísticas e da natureza do meio de investigação.

Na mesma lógica, igualmente despropositada em ambiente digital se manifesta a norma do art. 5º do RJAE, não se compreendendo qual o sentido em atribuir uma identidade fictícia, pelo menos nos moldes em que ela está legalmente prevista, a um agente que atua já de princípio por detrás de um aparelho eletrónico, de forma totalmente virtual e oculta. De facto, a ocultação de identidade do agente encoberto digital é o procedimento normal na interação com terceiros, pelo que não constitui algo inovador num contexto em que, como sabemos, o contacto é feito essencialmente através de identidades não reais. Assim, atendendo à teleologia da norma, não existe, em princípio, necessidade de previsão de criação de uma identidade fictícia ou, pelo menos, nos exatos termos em que está prevista no artigo 5º da Lei nº 101/2001. Na verdade, essencial se revelaria antes o balizamento do número e qualidade de identidades virtuais passíveis de ser atribuídas ao agente para cada concreta ação, algo que a Lei não faz.

Finalmente, mas não menos importante, também no que respeita à isenção de responsabilidade criminal do agente encoberto digital, reconhecemos que se o art. 6º do RJAE já levantava dúvidas nas clássicas ações encobertas, maiores problemas suscita neste novíssimo âmbito, tendo em conta as caraterísticas que o próprio ambiente digital apresenta e à forma inevitavelmente mais comprometida com que o agente necessita de se envolver no meio criminoso para nele poder aceder e penetrar.

Ora, atendendo a tudo o que atrás ficou dito, vários problemas detetámos na técnica legislativa adotada na regulação das ações encobertas digitais: se, por um lado, a aplicação analógica de determinados preceitos se revela desprovida de sentido, porquanto assistimos existir uma realidade sensivelmente diferente nas investigações que decorrem em ambiente digital das que se desenvolvem em ambiente físico, por outro, outras normas revelam-se francamente pouco densificadas para dar resposta a determinadas questões específicas que o mundo virtual convoca.

Acrescem ainda a estas situações de desajustamento legislativo problemas relativamente aos quais existe uma absoluta ausência de resposta. Por exemplo, tanto o art. 19º da LC como o RJAE são omissos no que a exigências de subsidiariedade no recurso a este método de obtenção de prova respeita. Por outro lado, o corpo legislativo existente

também nada especifica quanto ao que sucederá à prova que tenha sido produzida ilicitamente, isto é, fora dos limites previstos no art. 6º do RAJE.

Finalmente, cumpre ainda mencionar, em jeito de antecipação à última parte deste estudo, que a atual legislação nada prevê quanto ao campo de atuação em que as ações encobertas digitais se poderão desenvolver. Efetivamente, o atual regime limita-se a apresentar o rol de crimes relativamente aos quais o método de obtenção de prova poderá ser judicialmente autorizado, não fazendo qualquer referência aos canais de comunicação em que as exigências legais deverão ser menores e, consequentemente, onde poderá prescindir-se do apertado controlo judicial que se pretende nas ações encobertas formais. Note-se que, como veremos, esta questão acaba por se revelar fulcral na medida em que a divisão, em ambiente digital, das comunicações que se desenvolvem em canais «abertos» (isto é, de acesso livre e público), das que se desenvolvem em canais «fechados» (de acesso restrito, condicionado), terá consequências diretas ao nível da própria liberdade de atuação do agente, da ingerência nos direitos fundamentais dos sujeitos investigados que dela resulte e, por aí, da validade da prova produzida.[188]

[188] PELLUCCI, Frederico, *"A atuação dos Agentes…" Op. Cit.* Pg. 252

PARTE III: REGIME JURÍDICO FUTURO – "A LEI QUE DEVERÍAMOS TER"[189]: INVERSÃO DO PARADIGMA

6. O repensar do atual regime jurídico: um possível esboço da regulamentação das ações encobertas digitais

Depois de percorrido todo o RJAE e a LC, em específico, o seu art. 19º, e de esgrimidas todas as fragilidades que a nossa lei processual penal apresenta no que respeita especificamente às investigações criminais que decorrem em ambiente digital, cremos estar em condições para prosseguir com a defesa de uma reforma legislativa capaz de colocar término às dificuldades que, de resto, fomos já evidenciando.[190]

A regulamentação dos meios de obtenção de prova no âmbito da criminalidade informática no nosso ordenamento jurídico revelou-se, na verdade, algo já tardia: efetivamente, só em 2009 o legislador português previu meios de obtenção de prova destinados a regular especificamente a aquisição de prova digital, muito embora Portugal já tivesse assinado em 2001 a Convenção sobre o Cibercrime do Conselho da Europa.[191]

Por outro lado, como constata Armando Dias Ramos, desde que surgiu o RJAE, a 25 de agosto de 2001, poucas alterações legislativas se registaram. Dessas alterações apenas resultou a adição da alínea e) no art. 2º do RJAE, tendo as restantes alíneas mantido a mesma designação, embora situadas em letras diferentes. Não foi, portanto, introduzida qualquer alteração que fizesse referência às ações encobertas digitais, o que se revela incompreensível.

Efetivamente, se em 2001 as investigações criminais em ambiente digital poderiam ter ainda expressão irrelevante, em 2013 "já se tinha dado um passo de gigante" nesse sentido: por essa altura já se fazia sentir o massivo uso da Internet e a utilização de dispositivos informáticos, a qualquer momento e em qualquer lugar, pelo que não seria difícil perceber que rapidamente esse avanço na tecnologia se estenderia também ao próprio

[189] Título inspirado no texto: JOÃO CONDE CORREIA, *Prova digital… Op. Cit.*

[190] Cumpre apenas referir que uma tal "proposta legislativa" será aqui construída mediante a invocação dos concretos problemas e a apresentação de eventuais soluções. A metodologia por nós seguida, numa humilde tentativa de atender às especificidades da figura do agente encoberto digital, não visa a apresentação de verdadeiras novas normas jurídicas, razão pela qual as soluções não serão elencadas de forma contínua, mas antes construídas de forma sucessiva ao longo do presente capítulo.

[191] DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 39.

âmbito de investigação criminal, tendo, assim, o legislador perdido a oportunidade perfeita para legislar convenientemente sobre o disposto na Lei do Cibercrime, mormente na temática das ações encobertas.[192]

Também a nível europeu, o desempenho legislativo nesta matéria tem ficado muito aquém do que seria esperado: a nova Diretiva do Cibercrime, 2013/40/UE do Parlamento Europeu e do Conselho, que veio substituir a Decisão-Quadro 2005/ 22/ JAI, não fez qualquer referência a esta vertente digital das ações encobertas, limitando-se a criminalizar as interceções ilegais e as condutas perpetradas com recurso a *botnets*.[193]

Ora, a escassa legislação em matéria de ações encobertas digitais, agravada por um regime notoriamente desadaptado à realidade que lhe é inerente (em face das insuficiências resultantes da aplicação, por analogia ou por remissão, da LC ao RJAE) determinam a nossa crença em que a tutela jurídica do ambiente digital, com a consagração do agente encoberto digital como verdadeiro método de obtenção de prova em processo penal, só será possível mediante a criação de um espaço próprio de regulamentação das suas atividades, único caminho capaz de conferir credibilidade e força probatória às provas por si obtidas.

De facto, de acordo com David Silva Ramalho, uma análise atenta ao regime jurídico atual subjacente às ações encobertas digitais permite-nos inferir que as disposições processuais em matéria probatória estão pensadas, na sua generalidade, para a prova fisicamente visível, palpável ou audível, sendo, portanto, os meios de obtenção de prova legalmente previstos na nossa lei processual penal não mais do que o resultado de uma evolução jurídica testada empiricamente no ambiente físico.[194] Assim, nas palavras do autor *supra* referido, "independentemente do fim, interesse ou direito que cada norma processual visa tutelar ou do trajecto evolutivo que seguiu, a verdade é que, pelo menos aquelas que existem há mais de duas décadas, estão concebidas para uma realidade que não contempla o mundo digital."[195]

---

[192] ARMANDO DIAS RAMOS, *A prova digital… Op. Cit.* Pg. 155 e 156. Neste sentido, também em jeito de crítica, prossegue David Silva Ramalho: "(…) na verdade, em termos processuais, ressalvadas algumas alterações pontuais introduzidas pela Lei nº 59/98, o legislador processual penal apenas despertou para os novos problemas há menos de uma década, entre 2007 e 2009" *Cfr.* DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 240 e 241

[193] ARMANDO DIAS RAMOS, *A prova digital… Op. Cit.* Pg. 155.

[194] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 240.

[195] *Ibidem*.

Pelo exposto, estará assim reunido um conjunto de razões suficientemente plausíveis que nos permite avançar e nos transporta para o último ponto da nossa dissertação: a reflexão sobre um eventual novo espaço de regulamentação, próprio das ações encobertas digitais, verdadeiramente capaz de atender às especificidades do mundo virtual.[196]

Pensar num espaço de regulamentação próprio implicará, naturalmente, a densificação dos aspetos que consideramos ainda não estarem vertidos de forma satisfatória no corpo da Lei atual, sendo certo que a regulamentação dessas questões, atualmente omissas ou insuficientes, deveria operar ao nível do CPP. Assim, na linha do pensamento de Armando Dias Ramos, à semelhança do que sucede no ordenamento jurídico espanhol, todas as normas reguladoras da marcha processual da figura do agente encoberto (incluindo da recolha de prova) deveriam constar do CPP.[197]

6.1. Âmbito subjetivo ativo: densificação do conceito de agente encoberto digital

No ordenamento jurídico português, embora seja notória a intenção de introdução da figura do agente encoberto digital no contexto das investigações criminais, o que é facto é que continua a não existir uma previsão expressa da mesma no corpo da Lei, contrariamente àquilo que já sucede noutros ordenamentos jurídicos, como o espanhol.[198]

Com efeito, um primeiro esforço a concretizar residiria na adaptação da noção que está prevista para o agente encoberto físico às investigações que decorrem em ambiente digital. De facto, uma figura tão complexa é merecedora de uma noção legal mais especificadora do que aquela que está vertida no art. 1º do RAJE, de modo a melhor retratar a sua realidade e o seu *modus operandi.*

Neste sentido, o agente encoberto digital poderá ser definido, como já bem avançou F. Bueno de Mata, como o funcionário público ou terceiro particular que, voluntariamente e por decisão de uma autoridade judicial, se infiltra na Internet com recurso a aparelhos e

---

[196] Também no sentido da necessidade de regulação das atividades do agente encoberto digital através de Lei própria veio já pronunciar-se Jorge Bacelar Gouveia, atual presidente do Observatório de Terrorismo, que, em face da desatualização da legislação nacional no combate às mais recentes vagas de ciberataques, entende "estar na altura de criar uma lei para agentes infiltrados do cibercrime". Veja-se: https://expresso.pt/sociedade/2022-03-15-Esta-na-altura-de-criar-uma-lei-para-agentes-infiltrados-do-cibercrime-defende-presidente-de-Observatorio-de-Terrorismo-dcb13996 [Acesso em: 22 de março de 2022].
[197] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 254.
[198] *Ex vi* nº 6 do artigo 282 bis da LECrim.

dispositivos informáticos, com o objetivo de obter informações sobre os autores e respetivos modos de atuação em certas práticas ilícitas no mundo virtual e, dessa forma, recolher eventual prova incriminatória. Assim, a sua função reside em, ocultando a sua verdadeira identidade, estabelecer contactos virtuais e gerar a necessária confiança dos investigados e, por essa via, penetrar, por um período de tempo considerável, o núcleo criminoso.[199]

No que respeita a quem pode, em concreto, encetar a investigação numa ação encoberta vimos já que o RJAE, analogicamente aplicado ao agente encoberto digital, permite que as investigações sejam levadas a cabo por funcionários de investigação criminal ou por terceiro, de forma totalmente indiscriminada. Ora, uma tal hipótese, apesar de criticável por variadas razões, não deixa de revestir sentido, na medida em que, por vezes, o recurso a terceiros se mostra mais eficiente na recolha de prova incriminatória. Basta pensarmos nas situações em que o terceiro esteja integrado no meio criminoso ou possua especiais conhecimentos técnicos lhe permitam infiltrar-se em áreas virtuais que, de outro modo, permaneceriam inacessíveis aos funcionários da polícia.

No entanto, se é verdade o que atrás ficou dito, também é verdade que a assunção do papel de agente encoberto por um terceiro poderá revelar-se particularmente difícil, na medida em que a lei não limita essa possibilidade a eventuais (co)arguidos. Ora, como já avançámos em momento anterior[200], nessa hipótese, não vemos como seria possível ao terceiro a compatibilização das suas funções de agente com os direitos e deveres que lhe adviessem do seu estatuto processual de (co)arguido. De maneira que entendemos que a Lei deveria ser expressa no sentido de excluir a possibilidade de um terceiro (co) arguido encetar, ele próprio, a ação encoberta digital e levar a cabo, em sentido material, a investigação.

No limite, a aceitar-se a possibilidade de os (co)arguidos intervirem na investigação, deveriam apenas poder fazê-lo de forma indireta/passiva. Assim, ancorados no pensamento de David Silva Ramalho, consideramos que todo o terceiro que pretendesse efetivamente colaborar com a justiça poderia fazê-lo facultando voluntariamente as suas credenciais de acesso aos canais de comunicação às forças policiais que, por sua vez, assumindo ficticiamente a sua identidade, procurariam por produzir prova.[201] Ou, em última instância, caso a sua intervenção ativa se revelasse efetivamente necessária, a atuação do

[199] FEDERICO BUENO DE MATA, *El agente encubierto en Internet… Op. Cit.* Pg. 297.
[200] *Vide:* ponto 4. da Parte II.
[201] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 300.

terceiro deveria pautar-se estritamente pelas regras previamente definidas pelos OPC, devendo, nesse caso, ficar sujeita a um minucioso controlo.

Note-se ainda que se o terceiro cooperante permitir que os funcionários de investigação criminal façam uso da sua identidade *online,* os limites desse consentimento deverão ser respeitados: por exemplo, o terceiro pode consentir que o funcionário de polícia use a sua identidade apenas para enviar ou receber *emails*, fazer *uploads* de publicações ou fazer *downloads* de certos arquivos; bem como pode também permitir que comunique com operadoras de serviços *online* que distribuem, de forma ilegal, obras protegidas por direitos de autor. Nesses casos, se o funcionário policial usar a identidade do terceiro para se envolver numa qualquer outra atividade ou praticar qualquer outro ato para o qual o último não consentiu, tal deverá ser entendido como um extravasamento dos limites e do escopo do consentimento do terceiro. Ora, para evitar estas situações abusivas de verdadeira "apropriação da identidade" de terceiro, seria de extrema utilidade a concordância, por escrito, entre os OPC e o terceiro relativamente aos atos que o último consentisse no uso da sua identidade *online* pelo primeiro.[202]

De relevar que esta questão se reveste de grande importância tendo em conta que o fenómeno de "apropriação" da identidade acaba por ser bastante mais comum no mundo digital. De facto, os agentes encobertos clássicos (físicos) dificilmente conseguem se apropriar da identidade de terceiro em comunicações pessoais ou até mesmo telefónicas, visto ser complexa a reprodução da imagem ou da voz de outra pessoa, pelo menos de forma convincente. Já quando os agentes usam recursos *online* para se comunicar com outrem, todos se apresentam por detrás de um aparelho informático-digital, através de *usernames* ou *nicknames (*nomes de usuário) e de outros métodos não físicos, tornando-se assim o engano bastante mais fácil. Além disso, existem várias técnicas computacionais que podem auxiliar a falsificação de uma identidade eletrónica, na medida em que permitem que os agentes enviem informações que parecem ter vindo de um determinado usuário.[203] Daí a premência da regulamentação da questão dos atos abrangidos pelo consentimento do terceiro que aceite colaborar com os OPC. Dessa forma, estaria, por um lado, assegurado o sucesso das

[202] *Cfr.* DEPARTMENT OF JUSTICE, Online Investigative Principles for Federal Law Enforcement Agents, 1999. Pg. 50 a 53. Disponível em: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf [Acesso em: 14 de dezembro de 2021].
[203] *Ibidem.* Pg. 54 e 55.

investigações, ao mesmo tempo que se garantia o respeito pelo exigido pelo princípio da proporcionalidade no que ao âmbito subjetivo ativo da norma respeita.

Cumpre ainda mencionar quanto à possibilidade de participação de terceiro que juízo mais rigoroso deverá, ao invés, ser feito quanto à prova que seja obtida por particulares que, de forma autónoma e sem qualquer prévia autorização judicial, iniciam e desenvolvem as suas investigações na Internet, sem qualquer acompanhamento, e, posteriormente, a cedem livremente aos OPC competentes.[204]

Questão com semelhante relevo e também particularmente difícil tem sido a da admissibilidade do uso, em ações encobertas em ambiente informático-digital, de *cybercops* por terceiros. Sabemos que, nos dias de hoje, fruto do desenvolvimento tecnológico, a presença humana torna-se cada vez mais dispensável, sendo possível, no âmbito das investigações criminais, criar programas informáticos que substituem pessoas sem que quem esteja a ser alvo de escrutínio tenha consciência de que não interage com uma pessoa verdadeira, mas com um *robot.* Verdadeiramente paradigmático revelou-se, nesta matéria, o caso *Sweetie,* um caso real em que uma imagem virtual, tipo *robot*, criada por uma ONG (Terre des Hommes), simulando uma menina de nacionalidade filipina, de 11 anos de idade, permitiu atrair e identificar inúmeros pedófilos *online.* Embora a criação desta menina virtual tenha permitido identificar os IP's de mais de 1000 adultos provenientes de 71 países diferentes, que frequentavam salas de conversação o*nline* com o objetivo de visualizar vídeos e fotografias pornográficas de menores, a troco de quantias monetárias, colocou-se,

[204] Veja-se, a este respeito, o caso *United States v. Kline*, em que Bradley Willman, um particular que, sem qualquer autorização judicial, hackeou o computador de Ronald Kline e conseguiu ter acesso a provas verdadeiramente capazes de o condenar pela prática de crimes relacionados com pornografia infantil. Embora Ronald tenha vindo a ser efetivamente condenado, tendo-se concluído pela admissibilidade da prova produzida, por se ter entendido que Bradley não era um agente policial e, como tal, a proteção conferida pela quarta Adenda do ordenamento jurídico americano não se aplicaria à prova por si obtida, a verdade é que um tal argumento justificativo não procederia num ordenamento jurídico como o nosso. (*Apud* DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 300 e 301). Neste sentido, já entre nós, também paradigmático se revelou o caso Rui Pinto que, reputado por uns de *whistleblower* (denunciante) e por outros um criminoso e pirata informático (*hacker)*, trouxe para a opinião pública e para a política nacional e internacional o debate sobre os limites entre o interesse público das denúncias e a forma, eventualmente ilícita, como essas informações foram obtidas. (Veja-se, neste sentido, a notícia: https://desporto.sapo.pt/futebol/artigos/entenda-o-caso-football-leaks-e-o-papel-do-portugues-rui-pinto-2 [Acesso em: 20 de abril de 2022]). Casos como os apresentados permitem-nos concluir que, tendo em conta a forma como a nossa Lei se encontra formulada, por muito útil que certas condutas de particulares se revistam na denúncia de ilícitos criminais, "a verdade é que, quando a prova incriminatória, ainda que obtida por particulares bem-intencionados, seja subsumível à factispécie dos artigos 32º, nº 8, da CRP e 126º, nº 1, do CPP, deverá a mesma ter-se como proibida e inutilizável em processo penal". *Cfr.* DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 301.

entre outras questões[205], a legitimidade da ONG para levar a cabo uma tal intervenção sem qualquer autorização e/ou controlo judicial.

No que respeita a esta possibilidade é inegável que à utilização de máquinas robotizadas estão associadas inúmeras vantagens. Perante a existência de investigações que requerem uma atividade prolongada no tempo e o empenho de um grande esforço humano, a monotorização de certos crimes informático-digitais por máquinas virtuais torna-se menos dispendiosa e psicologicamente menos desgastante. Porém, a verdade é que, de acordo com Armando Dias Ramos, em face da atual redação do RJAE, essa possibilidade está arredada, na medida em que estipula expressamente, no seu art. 1º, nº 2, que são "ações encobertas aquelas que sejam desenvolvidas por **funcionários de investigação criminal** ou por **terceiros** atuando sobre o controlo da Polícia Judiciária".[206]

Ora, entre nós, tendo por base a redação do art. 1º/2 do RJAE, acompanhando o pensamento de Duarte Rodrigues Nunes, entendemos que o que a Lei prevê é que "as ações encobertas sejam realizadas por agentes policiais ou particulares sob o controlo das autoridades e não por particulares agindo *motu proprium*, pelo que, desde que o *Cybercop* seja controlado pelas autoridades, diretamente ou mediante o controlo do particular que controla o *Cybercop* (*v.g*., uma empresa que produza esses programas informáticos), não vemos em que medida a Lei não é observada".[207]

De facto, em determinados casos, não criamos obstáculos à possibilidade de terceiros desenvolverem programas informáticos, capazes de simular pessoas reais sem que os suspeitos investigados se apercebam de que não estão a interagir com pessoas verdadeiras, produzindo prova lícita e apta a ser valorada, desde que o façam sempre sob o controlo das autoridades judiciais. Assim, à semelhança da posição que manifestámos em relação à possibilidade em ser um (co)arguido a intervir numa investigação encoberta, também aqui entendemos que a admitir-se a possibilidade de utilização de *cybercops*, criados por terceiro, tal só seria, no limite, admissível se monitorizada junto dos OPC competentes. Note-se que,

---

[205] Poderia questionar-se, *ex ante*, se o facto de se tratar de uma boneca virtual e, portanto, estarmos perante uma tentativa inidónea da prática de um crime, por não existir uma vítima propriamente dita, determinaria a impossibilidade de aplicação de uma sanção penal. Porém, assumindo o desconhecimento dos sujeitos investigados de que não se tratava de uma pessoa real, o que deverá relevar será a análise da sua punibilidade em face da intenção verificada na prática do crime. Também neste sentido prossegue ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 236.

[206] *Cfr. Ibidem*. Pg. 226 (negrito nosso).

[207] DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 53.

embora Armando Dias Ramos não enverede pela sua admissibilidade, acaba por reconhecer que a utilização de c*ybercops* vai, no futuro, acabar por se tornar uma realidade. Nas suas palavras "o caminho da investigação na internet vai passar obrigatoriamente pela inclusão de c*ybercops* que irão realizar diligências de investigação na internet, sob diversas formas, na qual se se inclui a do agente encoberto…".[208]

Finalmente, ainda no que à definição de agente encoberto digital respeita, cumpre apontar um último problema. De acordo com F. Bueno de Mata, a lei processual espanhola que regula as atividades do agente encoberto digital padece de fortes insuficiências por não elencar as caraterísticas essenciais que todo o funcionário ou terceiro deveria apresentar para poder assumir as vestes de um agente encoberto digital. Ora, olhando para a nossa legislação atual denotamos que um tal problema acaba também se encontrar no nosso ordenamento jurídico.

De facto, o legislador processual português não procedeu à enunciação das caraterísticas especiais que, naturalmente, um agente encoberto virtual deve apresentar, pelo que, ancorados no pensamento do autor *supra* referido, entendemos que os critérios de seleção deverão ser enunciados, de forma expressa, no texto da Lei.

Deste modo, estando em causa um agente encoberto digital consideramos que não revestem de particular importância as caraterísticas que estejam relacionadas com a imagem física do agente (*v.g.* estado civil, idade, físico ou aparência), antes se assumindo essenciais as suas qualidades psicológicas como sejam a empatia, a confidencialidade, autonomia e capacidade para tomar decisões consoante as exigências concretas de cada uma das situações com se depare no exercício das suas funções. A essas caraterísticas pessoais, obviamente acresceriam os necessários conhecimentos informáticos para encetar a infiltração virtual.[209] Ademais, o agente encoberto deverá apresentar uma "pegada digital" suficientemente forte, isto é, "um histórico credível e sedimentado na Internet e que seja compatível com a personalidade que assumirá na ação encoberta"[210], essencial para garantir o sucesso das suas operações.

---

[208] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 227.

[209] FEDERICO BUENO DE MATA, *El agente encubierto en Internet… Op. Cit.* Pg. 300 e 301.

[210] DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 54; Armando Dias Ramos aponta a pegada digital como um entrave à utilização do agente encoberto na era informática, na medida em que o sucesso da ação encoberta digital requer que o agente detenha um histórico na internet, isto é, um passado suficientemente credível ligado à prática de crimes, não só a nível de perfis nas redes sociais, mas também noutras plataformas como blogues e fóruns. A criação de uma verdadeira pegada digital não é algo que se

6.2. O catálogo de crimes: a necessidade de redução da sua amplitude

Uma outra questão problemática facilmente percetível pela análise de que nos ocupámos do art. 2º, nº 1 do RJAE e do art. 19º, nº 1 da LC, preceitos responsáveis pela delimitação do âmbito subjetivo das ações encobertas digitas, prende-se exatamente com a amplitude do catálogo de crimes.

De facto, atento o nº1 do art. 19º da LC, a presença de uma "associação inopinada entre crimes informáticos, crimes cometidos através de um sistema informático e acção encoberta"[211] tem constituído motivo para se apontar que o preceito se releva desmedido, com a ampliação da investigação oculta em ambiente digital a um leque muito vasto de crimes.

De outro prisma, também a própria discrepância que o art. 19º da LC apresenta em face do art. 2º do RJAE no que respeita ao catálogo de crimes admitido não tem escapado à crítica de considerável doutrina, justificando-se, nas palavras de Duarte Rodrigues Nunes, "uma maior similitude entre os catálogos do art. 2º da Lei nº 101/2001 (e do art. 188º, nº2, da Lei nº 23/2007, de 4 de julho) e do art. 19º, nº1 da Lei nº 109/2009, sem prejuízo da inserção dos crimes previstos nesta Lei quanto às ações encobertas em ambiente informático-digital."[212]

Também neste sentido parece apontar Susana Aires de Sousa que, sufragando-se do exemplo dos crimes contra a liberdade e autodeterminação sexual, nos demonstra existir um claro desencontro entre os dois Diplomas. De acordo com esta Autora, o RJAE determina que as ações encobertas só estão legitimadas quando o crime a ser investigado seja punível com pena superior a 5 anos, não relevando o facto de o menor ter idade inferior a 16 anos; já na LC a legitimação da investigação de um crime desta índole que tenha sido praticado em ambiente informático não está dependente da concreta pena que lhe seja aplicável. Do que resulta que a ação encoberta física tenha um âmbito de aplicabilidade sensivelmente menor, só podendo ser desencadeada quando em causa esteja um crime sexual contra menor

consiga fazer de forma instantânea, requerendo uma atividade prolongada no tempo. Como exemplifica o Autor, não basta efetuar publicações com datas anteriores ou criar histórias em páginas w*eb* diferentes, pois há sempre possibilidade de verificar se as mesmas foram efetivamente publicadas naquelas datas e aferir a sua veracidade. *Cfr*. ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 86.

[211] PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 126.

[212] DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Cit*. Pg. 206 e 207.

de 16 anos, punível com pena superior a 5 anos; ao passo que a ação encoberta digital, diferentemente, pode ser aplicada sempre que em causa esteja a investigação de um qualquer crime doloso contra a liberdade ou autodeterminação sexual de menor com idade compreendida até aos 18 anos.[213]

Note-se que, em face do exposto, existindo um âmbito de aplicabilidade muito maior nas ações encobertas digitais, a norma chega a revelar-se perigosa pois permite o desencadeamento de «*quaisquer*»[214] investigações no âmbito de ilícitos digitais para os quais estão previstas penas relativamente baixas e de gravidade mediana. Ora, atendendo às caraterísticas gerais das ações encobertas digitais, um método oculto de investigação por excelência, com sérias repercussões no âmago dos direitos, liberdades e garantias dos sujeitos investigados, justificar-se-ia uma maior contenção na extensão da sua aplicabilidade, tendo em conta as exigências dos princípios da proporcionalidade e da necessidade.

Deste modo, consideramos, na linha de Paulo Dá Mesquita, não ser justificável, do ponto de vista jurídico-constitucional, que um método oculto de investigação criminal desta natureza seja estendido a crimes como os previstos nos arts. 3.º, n.º 1 (falsidade informática), 5.º, n.ºs 1 e 2 (sabotagem informática), 6.º, n.ºs 1 e 3 (acesso legítimo), e 7.º, n.ºs 1 e 2 (interceção ilegítima), todos da Lei n.º 109/2009, aos crimes dolosos puníveis com penas inferiores a 5 anos de prisão referidos no art. 19.º, n.º 1, al. b), bem como aos crimes negligentes que sejam puníveis com pena superior a 5 anos de prisão, sem mais exigências. Nas palavras do Autor *supra* citado, a norma "transgride, claramente, a linha do admissível, ao prever uma medida de carácter muito excecional para um leque muito amplo de crimes".[215]

Pedro Dias Venâncio acrescenta ainda que o catálogo da norma se revela algo curioso, na medida em que prevê a proteção de crimes contra obras protegidas, mas não de crimes relativos à proteção das medidas de caráter tecnológico e das informações para a gestão eletrónica dos direitos[216], que seria merecedora de igual tratamento jurídico-penal.

---

[213] SUSANA AIRES DE SOUSA, *Ações encobertas … Op. Cit.* Pg. 38 (nota de pé de página nº11).
[214] PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 126;
[215] *Ibidem;* Em sentido idêntico prossegue Paulo Pinto de Albuquerque que, tecendo severas críticas à amplitude da norma, defende a redução do seu catálogo. *Cfr.* PAULO PINTO DE ALBUQUERQUE, *Comentário ao código de processo penal à luz da constituição da República e da Convenção Europeia dos Direitos do Homem.* 4. Ed. Lisboa: Ed. Universidade Católica, 2011. Pg. 681 e 682.
[216] PEDRO DIAS VENÂNCIO, *Lei do Cibercrime Anotada e Comentada* [Art. 19º]. Coimbra: Coimbra Editora, 1ª Edição, janeiro de 2011. Pg. 122.

6.3. Os concretos "meios e dispositivos informáticos"

No que respeita aos concretos meios e dispositivos informáticos de que, eventualmente, o agente encoberto digital possa necessitar de se socorrer nas suas atividades investigativas, estipula-se no nº 2 do art. 19º da LC que se "*observam, naquilo que for aplicável, as regras previstas para a intercepção de comunicações."* Assim, assiste-se aqui novamente à utilização da mesma técnica legislativa analógica, continuando o legislador a limitar-se a remeter a regulação das ações encobertas digitais para outros métodos de investigação já com um espaço próprio de regulamentação no CPP, ínsitos nos seus artigos 187º a 189º, sem qualquer outro enquadramento.

Ora, esta aplicação *mutatis mutandis* do regime jurídico previsto para a interceção de comunicações aos "meios e dispositivos informáticos" utilizados no âmbito das ações encobertas digitais tem suscitado dúvidas e tem vindo a ser alvo de inúmeras críticas, apontando-se nomeadamente que apenas veio contribuir para o aprofundamento da incongruência sistemática já introduzida pelo nº1 do art. 19º.[217]

Entre nós, a adequação da aplicação do regime que está previsto para a interceção de comunicações só poderá ser aferida mediante a análise da forma como os crimes informático-digitais são praticados. É consabido que estes crimes são, na sua maioria, praticados com recurso a técnicas de anonimização, não sendo possível conhecer o IP da ligação da Internet com que os criminosos atuam. Em face desta dificuldade, Armando Dias Ramos aponta: "desconhecendo-se o IP dos autores/suspeitos dos factos será difícil, se não mesmo impossível, realizar uma interceção das comunicações, como estipula o nº2 do art. 19º da LC. E ainda que fosse conhecido um IP nacional como se poderia aplicar o regime do art. 187º do CPP, se este apenas prevê um catálogo fechado de alvos?[218]". Assim, acompanhando o Autor *supra* citado, aqueles argumentos poderão constituir uma primeira motivação para justificar as insuficiências que decorrem da mera aplicação, por remissão, do regime da interceção de comunicações às ações encobertas que se desenvolvem em ambiente digital.

De facto, como bem evidencia Armando Dias Ramos, mesmo na hipótese de ser conhecido o IP, não podemos perder de vista que o suspeito poderá na sua prática criminosa

[217] PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 127
[218] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 181.

estar a fazer uso da ligação de Internet de alguém sem qualquer conexão com o crime ou de um *acess point* público disponibilizado por uma entidade pública ou privada. Note-se que no caso de uma escuta de dados a ligação que sai para o exterior é igual para todos os elementos de uma família ou grupo de pessoas que se ligue ao *router* da internet, sendo esse IP que será identificado pelos operadores de comunicações.[219]

Por outro lado, para além dos problemas anteriormente apontados, a (in)coerência da aplicação *mutatis mutandis* do regime jurídico previsto para a interceção de comunicações às ações encobertas digitais poderá também ser percecionada pela análise da sua (in)suficiência na resposta às especificidades que as últimas convocam.

Ora, como já foi evidenciado, a LC considera bastante para a regulamentação da utilização, no âmbito das ações encobertas digitais, dos meios e dispositivos informáticos as regras que estão previstas para a interceção de comunicações. De acordo com a definição constante do art. 2º/e) da Proposta de Lei nº 289/X/4 – Lei do Cibercrime –, por «interceção» entende-se ser o "ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros". Neste sentido, Armando Dias Ramos completa a definição encetando que "intercetar significa intrometer de permeio, ou seja, entre o emissor e o recetor alguém consegue captar todo o conteúdo das comunicações eletrónicas"[220] e, semelhantemente, Dá Mesquita, aponta ser o ato destinado à recolha de informações armazenadas num sistema informático através de um dispositivo eletrónico.[221]

Posto isto, atendendo à definição de agente encoberto, patente no art. 1º/2 do RJAE (para a qual remete o art. 19º da LC aqui em análise), definido como o funcionário de investigação criminal ou terceiro que, atuando com ocultação da sua qualidade e identidade e sob o controlo da Polícia Judiciária, dedica-se à prevenção e repressão dos crimes catalogados, parece-nos que, envolvendo a sua operação múltiplas formas de atuação e práticas complexas, poderá revelar-se redutora a remissão das ações encobertas digitais a uma mera e simples interceção de comunicações - uma entre muitas outras formas específicas de investigação que aquele método oculto de obtenção de prova abrange.

Com efeito, a função do agente encoberto digital é, de facto, muito mais ampla que a mera interceção de comunicações: para além de intercetar comunicações, o agente cria

[219] *Ibidem.* Pg. 181.
[220] ARMANDO DIAS RAMOS, *A prova digital… Op. Cit.* Pg. 156
[221] PAULO DÁ MESQUITA, *Processo Penal… Op. Cit*. Pg. 120.

uma aparência virtual através de uma identidade fictícia, de maneira a ocultar a sua qualidade e identidade real, procura envolver-se no meio criminoso, estabelecer contactos com os suspeitos investigados, conquistar a sua confiança e, por essa via, recolher eventual prova incriminatória. Trata-se, pois, de uma investigação francamente mais complexa, que exige técnicas e modos de intervenção variados e, portanto, não reconduzíveis a uma mera interceção que, quando telefónica, poderá ser bem-sucedida sem sequer ser necessária qualquer ocultação da qualidade do agente ou da sua identidade.[222]

Assim, como bem evidencia Armando Dias Ramos, "quando se efetua uma interceção telefónica, regime previsto no CPP, para onde somos levados obrigatoriamente pelo legislador na Lei do Cibercrime, não existe qualquer ocultação da qualidade do agente da sua identidade, apenas se trata de um procedimento técnico em que se consegue "escutar" a comunicação, seja ela telefónica ou de dados informáticos".[223] De maneira que para proceder a uma interceção de comunicações não será necessário recorrer à figura do agente encoberto digital, bastando a solicitação aos operadores de comunicações da respetiva interceção, depois de devidamente obtida a autorização do Juiz.[224]

Cumpre ainda relevar que a análise da opção metodológica de adaptação dos conceitos já existentes a novas realidades, como sucede neste âmbito, permite-nos detetar ainda outras incongruências: observámos já que a norma consagra a admissibilidade do recurso a "meios e dispositivos informáticos" no âmbito das atividades do agente encoberto. A esses "meios e dispositivos informáticos" é aplicável o regime da interceção de comunicações e, por sua vez, o das escutas telefónicas (por via de remissão daquele), do que resulta o cruzamento legal de três regimes cuja natureza, na verdade, se revela completamente diferente e até dissonante. Vejamos, desde logo, do ponto de vista das garantias processuais do arguido e da publicidade do meio de obtenção de prova utilizado: enquanto o RJAE não garante ao arguido o conhecimento de que foi alvo de uma investigação dessa índole, o regime das escutas telefónicas, prevê, no seu artigo 188º nº8 (aplicável por força do art. 18º nº4 da LC) a possibilidade de o arguido examinar os suportes técnicos das conversações e de ter acesso, caso pretenda juntar ao processo, à cópia dessas conversações bem como dos relatórios efetuados pelos OPC. Em face disto, como refere

---

[222] Neste sentido, ARMANDO DIAS RAMOS, *A prova digital… Op. Cit.* Pg. 156 e 157.
[223] ARMANDO DIAS RAMOS, *A investigação do Cibercrime – Nótulas sobre o paradigma legislativo atual e a realidade tecnológica, in Cyberlaw by CIJIC,* Edição nº VIII, setembro de 2019. Pg. 52.
[224] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 184.

David Silva Ramalho, se entendermos a remissão do artigo 19.º, n.º 2, para o artigo 18.º, ambos da Lei do Cibercrime, como incluindo a remissão para o regime das escutas telefónicas do artigo 188.º do CPP, poderemos cair no absurdo de não ser divulgada ao arguido a existência de uma ação encoberta, mas, simultaneamente, de terem de lhe ser facultados os suportes técnicos nos quais se encontra armazenada a prova recolhida através dela.[225] De notar que, ainda na linha do pensamento do Autor, esta incompatibilidade não poderá servir de fundamento à prevalência da regra prevista no RJAE de exclusão da publicidade dos concretos meios e dispositivos informáticos utilizados num determinado procedimento criminal, na medida em que, atuando o agente encoberto digital num ambiente, à partida, mais seguro do ponto de vista da sua segurança pessoal, e, portanto, inexistindo razões para fundamentar o secretismo das suas atividades, deverá o arguido ter conhecimento das diligências investigativas que contra si correram em sede de instrução, sob pena de se violar uma das suas mais básicas garantias processuais de defesa.[226]

Pelo exposto, está reunido um conjunto considerável de razões que nos permite concluir "que [a] interceção de comunicações e ações encobertas são figuras distintas de investigação criminal, com catálogos de crimes diferentes e formalidades das operações inigualáveis"[227], não restando dúvidas que a articulação entre os regimes que estão subjacentes à regulação das ações encobertas digitais revela sérias dificuldades.

Por outro lado, da análise que fizemos já em momento anterior[228], foi possível verificar que os "*meios e dispositivos informáticos*" a que a norma faz referência no seu nº2 não se subsumem a qualquer um dos meios de obtenção de prova previstos na legislação processual penal portuguesa. De facto, esta é uma conclusão que se impõe pela circunstância de o legislador ter sentido necessidade de introduzir uma norma nova para legitimar o recurso àqueles meios e dispositivos informáticos. Note-se que a própria letra da lei esclarece que o regime que está previsto para a interceção de comunicações apenas é aplicável às ações encobertas digitais apenas e só naquilo que lhes for conveniente ("*observam-se, **naquilo que for aplicável**[229], as regras previstas para a interceção de comunicações.").*[230]

[225] DAVID SILVA RAMALHO, *O uso de malware… Op. Cit.* Pg. 235.
[226] *Ibidem.*
[227] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit*. Pg. 184.
[228] *Vide:* ponto 3. da Parte II.
[229] Negrito nosso.
[230] DAVID SILVA RAMALHO, *O uso de malware… Op. Cit.* Pg. 230.

Posto isto, questionamo-nos: que meios e dispositivos informáticos estarão aqui em causa? A resposta a esta questão não se reveste de simplicidade. Numa interpretação mais atualista da norma há quem considere que, por um lado, poderá ter sido a válvula de que o legislador se serviu para consagrar a admissibilidade da realização de buscas *online* no âmbito das ações encobertas[231]; e, por outro, há quem vá mais longe e entenda que o preceito pretendeu consagrar a utilização de *malware*[232] como método oculto de investigação criminal em ambiente digital.[233]

De facto, a forma como a norma se encontra estruturada sugere que tenhamos em consideração outros meios e dispositivos informáticos que não encontram regulação na nossa lei processual penal, mas que por terem semelhante "carácter excecional, invasivo e insidioso possa ser comparado e condicionado ao recurso ao agente encoberto e cujo funcionamento possa ser regulado e limitado pelo regime da interceção de comunicações".[234]

Note-se que, como evidencia David Silva Ramalho, a terminologia adotada pelo legislador português é muito semelhante à utilizada em outros ordenamentos jurídicos para consagrar o *malware* (o Autor socorre-se, entre outros, do exemplo do ordenamento jurídico francês que, no artigo 706-101-1 do seu CPP, utiliza uma designação análoga à nossa – "*dispositivos técnicos*").[235] Ressalva, porém, o Autor *supra* citado que, apesar dos benefícios

---

[231] JOÃO CONDE CORREIA, *Prova digital… Op. Cit.* Pg. 42;

[232] Expressão que diz respeito a "todo o tipo de programas instalados sub-repticiamente por terceiros num sistema informático que podem ser utilizados para, de algum modo, comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao sistema informático infetado, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos*". (Cfr.* DAVID SILVA RAMALHO, *O uso de malware… Op. Cit.* Pg. 202.) Juliana Campos acrescenta que o *malware* corresponde a um programa informático que é instalado ocultamente no sistema informático do visado, para recolha de prova interna e/ou externa ao sistema informático, quando aquele comporte a ativação de *hardware. (Cfr.* JULIANA FILIPA SOUSA CAMPOS, *O Malware como Meio de Obtenção de Prova em Processo Penal*, Coimbra: Edições Almedina, 2021. Pg. 27.) De relevar que, todavia, o *malware* não se confunde com as ações encobertas digitais, na medida em que o primeiro se traduz num método passivo de recolha de informações, ao passo que nas segundas há uma interação propriamente dita entre os funcionários de investigação criminal ou o terceiro com os suspeitos investigados, que permite o acesso a informações, planos e confidências. (*Cfr. Ibidem,* Pg. 94). Por se tratar de uma forma de investigação cuja complexidade acarretaria desenvolvimentos maiores, limitar-nos-emos a fazer-lhe uma breve referência, sob pena de extravasarmos os limites subjacentes à temática do nosso estudo.

[233] Contra esta possibilidade se insurge Juliana Campos, que considera inexistir qualquer base legal que, pelo menos de forma expressa, legitime o uso de *malware,* conjugado com o facto de colidir em toda a sua plenitude com as finalidades do processo penal e com o princípio da interpretação conforme à Constituição. No seu entender, está em causa um meio com um elevado potencial de dessava de direitos, liberdades e garantias, pelo que só uma lei expressa, clara e determinada poderá legitimar a sua utilização. Ademais, na sua ótica, o *malware* constitui um meio de obtenção de prova autonomizado das ações encobertas, pelo que a sua legitimação ao abrigo do nº2 do art. 19º da LC nunca poderia ser possível. *Cfr. Ibidem.* Pg. 80; 96 e 97.

[234] DAVID SILVA RAMALHO, *O uso de malware… Op. Cit*. Pg. 231.

[235] *Ibidem*. Pg. 231.

que uma investigação desta índole poderia trazer para o processo, a verdade é que o uso de *malware* não está expressamente legitimado e admiti-lo à luz do art. 19º, nº2 da LC seria incompatível com os princípios constitucionais ínsitos nos art. 26º nº1 e 2 e 32º nº4 da CRP. Ademais, entende o Autor que não deverá ser, sem mais, legitimado este método de investigação, sobretudo quando em causa esteja a prossecução de finalidades preventivas, na medida em que se, por um lado, estas ações no âmbito da prevenção criminal poderiam aparentar ser admissíveis ao abrigo do disposto no artigo 3º, nº4 do RJAE, por outro, o artigo 18º nº2 da LC deixa claro que tanto a interceção como o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, isto é, depois de iniciadas as investigações no âmbito de um processo-crime.[236]

Semelhantemente a David Silva Ramalho posiciona-se Armando Dias Ramos, embora o último defenda uma terminologia diferente: no seu entender, o nome do s*oftware* utilizado para fins de obtenção de prova digital deverá antes receber a designação de *"benware"* – e não de "*malware"* – uma vez que a esta última está associada uma conotação negativa (traduzida à letra "sistema maligno"), incompatível com a finalidade do processo penal de realização da justiça (o que implica, naturalmente, meios benéficos nessa prossecução e que exista uma vigilância apertada sobre a sua utilização).[237]

Entre nós, na linha do Autor anterior, reconhecendo a necessidade de se recorrer a estas formas de investigação para se fazer face à criminalidade informático-digital, entendemos que o envio de *benware,* expressão igualmente preferível para nós, através de redes de informação e comunicação deveria ser consagrado de forma expressa no corpo da lei, legitimando-se, por essa via, a observação do que existe no dispositivo informático do sujeito investigado, bem como a captura do som ou de imagem no âmbito de uma ação encoberta, muito embora tal técnica de investigação sempre ficasse sujeita à autorização judicial do JIC e a um despacho por ele emanado devidamente justificado.[238]

Já no que respeita à possibilidade de cumulação das ações encobertas digitais com a utilização de vários meios técnicos, nos quais se inclui obviamente a interceção de

---

[236] *Cfr. Ibidem.* Pg. 232. Nota de pé de página nº 118.

[237] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 208

[238] *Ibidem*. Pg. 257; De relevar que, no ordenamento jurídico espanhol, a LECrim autoriza expressamente, no art. 588 septies a., nº1, o agente encoberto a enviar ficheiros com software específico, sem que o suspeito disso se aperceba, com o objetivo de localizar e recolher ficheiros ilícitos e, dessa forma, produzir eventual prova incriminatória. Tal medida de investigação não poderá ter, no entanto, uma duração superior a 1 mês, prorrogável por iguais períodos, até um máximo de 3 meses. *Cfr. Ibidem.* Pg. 206 e 207.

comunicações, consideramos que tal sempre seria admissível, na exata medida em que o êxito das investigações neste ambiente e em relação a certos tipos-legais de crime depende em larga medida da utilização – por vezes, cumulativa – de vários métodos de obtenção de prova, por regra, todos eles restritivos de direitos fundamentais.[239] Neste sentido, Duarte Alberto Rodrigues Nunes envereda pela admissibilidade de cumulação das ações encobertas digitais com outros meios de obtenção de prova não subsumíveis ao nº2 do art. 19º da LC, como é o exemplo a pesquisa de dados informáticos e sua posterior cópia, desde que seja respeitado o princípio da proporcionalidade e da proibição de excesso.[240] No entanto, ressalva que essa cumulação só será possível se não implicar uma "vigilância total", isto é, não tenha como consequência a obtenção, de forma prolongada no tempo e através do uso de medidas de observação, de informações relativas à totalidade da vida do concreto visado.[241] Entre nós, admitindo, que a questão não possa ser tomada de forma tão pacífica, a sua regulamentação afigurar-se-nos-ia essencial, de maneira a não ferir o princípio da legalidade. De facto, um método excecional de investigação exige maiores especificações legais, sob pena de se correr o risco de cairmos no domínio das provas proibidas (nos exatos termos do nº 3 do art. 126º CPP).

Note-se que quando falamos da necessidade de uma regulamentação mais clara e precisa quanto à pesquisa de dados informáticos, referimo-nos também às pessoas cujos dados podem ser alvo de uma investigação digital e recolhidos para efeitos de prova.[242] Embora haja quem apele à aplicação analógica do preceituado no art. 187º/4 do CPP[243], permitindo-se assim, amplamente, no âmbito das ações encobertas digitais, a interceção e a gravação de dados informáticos do arguido, do suspeito, do intermediário ou da vítima,

---

[239] *Cfr.* DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Cit*. Pg. 209.
[240] *Ibidem.* Pg. 202.
[241] DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 58.
[242] Semelhantemente ao aqui pugnado por nós, Juliana Campos avança, na almejada regulação do *malware,* com a necessidade de a lei determinar um "catálogo de pessoas" relativamente às quais aquela forma de investigação pudesse ser utilizada. No seu entender, poderia ser nela incluída o suspeito, o arguido ou outras pessoas que o preceito normativo entendesse convenientes. Alerta a Autora para o facto de, nesse caso, a aferição desse requisito normativo material, podendo deparar-se com elementos de identificação mínimos, como n*icknames, usernames ou emails (*dificuldade também perfeitamente extensível às ações encobertas digitais), apenas se exigiria que a pessoa que estivesse a usar um daqueles elementos se enquadrasse no catálogo previsto na lei, ainda que "referenciada" numa fase prévia da investigação através de um daqueles elementos. Assim, o essencial residiria na necessidade de o alvo encontrar correspondência no catálogo em virtude de através dele existir uma alta probabilidade de ser recolhido material ilícito incriminatório, afastando-se, desse modo, aquilo que a Autora denomina de "*fishing expeditions"*, isto é, verdadeiras "pescas" de agentes da prática de crimes. *Vide:* JULIANA FILIPA SOUSA CAMPOS, *O Malware… Op. Cit.* Pg. 161 e 162; No mesmo sentido: DUARTE ALBERTO RODRIGUES NUNES*, Os meios de obtenção… Op. Cit.* Pg. 208.
[243] Neste sentido, DUARTE ALBERTO RODRIGUES NUNES*, Os meios de obtenção… Op. Cit*. Pg. 222.

acreditamos que nem sempre isso deverá ser admissível, pelas mesmas razões *supra* invocadas. Efetivamente, um método oculto de investigação criminal, com repercussões sérias nos direitos, liberdades e garantias daqueles que dele sejam alvo, deverá estar reservado para situações excecionais.

Finalmente, questão igualmente importante, relacionada com os limites à prova recolhida através destes "meios e dispositivos informáticos" prende-se com a possibilidade de utilização de conhecimentos fortuitos no âmbito de uma ação encoberta. David Silva Ramalho entende que, por exemplo, na hipótese de, no decurso de uma investigação criminal por suspeita da prática de um crime de pornografia de menores (previsto e punido pelo art. 176º do CP) ser encontrada prova de que o visado apenas utilizava uma versão pirateada do sistema operativo, subsumível ao crime de reprodução ilegítima de programa protegido (nos termos do art. 8º da LC), a sua valoração dependerá da verificação, em concreto, da proporcionalidade do método utilizado se o ilícito que foi descoberto tivesse sido aquele que inicialmente tinha motivado o seu recurso. Assim, se o recurso ao meio de obtenção de prova se revela proporcional ao ilícito descoberto, a prova deverá ser valorada; caso contrário, ter-se-á como proibida por violar o princípio da proporcionalidade.[244]

Ora, entre nós, embora os preceitos que se dediquem à regulação das atividades do agente encoberto digital não regulem esta questão, revelando mais uma clara insuficiência legislativa nesta matéria, tomando por base o preceituado no seu art, 3º, nº1 do RAJE, que exige a identificação, em concreto, dos fins que se pretende alcançar com a ação encoberta, parece-nos, na linha de Armando Dias Ramos, que a utilização de conhecimentos fortuitos obtidos durante a investigação será suscetível de ferir o plasmado no art. 18º da CRP, nas suas dimensões da necessidade, subsidiariedade e proporcionalidade em sentido estrito. Para esse entendimento concorre, por um lado, o facto de, a ter sido essa a intenção do legislador, já se teria alargado expressamente o efeito dos conhecimentos fortuitos às ações encobertas e, por outro lado, a falta de controlo judicial que resultaria da admissibilidade de uma investigação deste tipo.[245]

[244] *Cfr*. DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 256 a 258.
[245] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit*. Pg. 109 a 111.

6.4. Da possibilidade de prossecução de finalidades preventivas e da competência para a sua iniciativa e decisão

Constatámos já que, no que respeita especificamente às ações encobertas que se desenvolvem em ambiente digital, o legislador limita a investigação aos crimes a que se refere o art. 19º/1 da Lei nº 109/2009 (e que não constam do art. 2º da Lei nº 101/2001) à prossecução de finalidades repressivas; já quanto aos crimes que constam do art. 2º do RJAE, o legislador não é claro, na medida em que admite o recurso a ações encobertas (quer para fazer face a fins preventivos, quer a fins repressivos) mas não identifica o tipo a que se refere: se apenas e exclusivamente às ações encobertas clássicas (físicas) ou se também às ações encobertas digitais, aqui agora em análise.[246]

Deste modo, não havendo uma discriminação na letra da lei, consideramos que a prossecução de finalidades preventivas se poderá estender às ações encobertas digitais, muito embora a prevenção criminal esteja apenas expressamente prevista para os casos que em causa esteja a prática de crimes que constam do art. 2º da Lei nº 101/2001.[247]

Entre nós, atento o tipo de criminalidade que servem, não obstante as ações encobertas deverem prosseguir fundamentalmente finalidades repressivas, não podemos deixar de reconhecer que elas também poderão ser eficazes na prevenção criminal, visto que permitem, quiçá, evitar a consumação, pelos mesmos agentes, de outros factos futuros da mesma natureza (ou de natureza análoga) de outros já praticados.[248] Note-se que, atento o plasmado no art. 272º, nº 3 da CRP, a função de prevenção dos crimes está contida nas atribuições da PJ, ainda que com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos. Assim, à semelhança de Armando Dias Ramos, entendemos que o futuro das atividades investigativas do agente encoberto digital deverá passar pelo deslindamento e prevenção da prática de crimes informático-digitais em casos devidamente sinalizados, justificados e de especial complexidade de investigação.[249]

---

[246] *Vide:* ponto 4.2. da Parte II.

[247] Idêntico entendimento parece-nos ter DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade… Op. Cit.* Pg. 855.

[248] Socorrendo-nos das palavras de Paulo Dá Mesquita, "no quadro da sociedade de risco é importante reconhecer que a prevenção primária e a segurança assumem reforçada relevância e determinam que se torne necessário ponderar a uma nova luz o recurso a meios limitadores dos direitos fundamentais, na defesa relativamente a perigos gerados pela criminalidade organizada ou pelos atentados contra os fundamentos do Estado". *Cfr.* PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 440.

[249] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 250.

Deste modo, tomando por base o princípio da lealdade[250], consideramos ser admissível o recurso à figura do agente encoberto digital na prossecução de finalidades preventivas sempre que " a inteligência dos agentes da Justiça ou os meios e a criminalidade ponha gravemente em causa os valores fundamentais que à Justiça Criminal cabe tutelar"[251].

De facto, reduzirmos as ações encobertas digitais à possibilidade de prossecução de finalidades meramente repressivas seria admitir, nas palavras de Duarte Alberto Rodrigues Nunes, a "inutilizabilidade prática deste tipo de ações encobertas"[252]. Ou, ainda, de outro prisma, admitir discriminações entre as ações encobertas "clássicas" e digitais no que respeita ao tipo de finalidades prosseguidas (repressivas ou preventivas) seria compactuar com a introdução de uma "descontinuidade perfeitamente desnecessária e evitável na nossa ordem jurídica e incompatível com a presunção de que o legislador goza nos termos do art. 9º, nº 3 do Código Civil."[253]

Por outro lado, a possibilidade de prossecução de finalidades preventivas no âmbito das ações encobertas digitais acaba por se impor até pela natureza das coisas. Um dos obstáculos mais decisivos na recolha de prova da prática de ilícitos em ambiente digital é a identificação do seu autor, sendo muito comum a dissimulação do IP do equipamento através do qual são praticados crimes cibernéticos, mediante a utilização de s*oftwares es*pecíficos através da *Dark Weeb,* como servidores *Proxys[254], Botnets[255] e VPN's (Virtual Private*

---

[250] Entendido como uma "maneira de agir no desenvolvimento da atividade processual em conformidade com o respeito dos direitos e da dignidade de todas as pessoas que participam no processo e com os deveres funcionais", constituindo assim "o fundamento do que a nossa lei processual qualifica como métodos proibidos de prova e proibições de prova (art. 32º, nº 8, da CRP, e art. 118º, nº 3, e 126º) ". *Cfr.* GERMANO MARQUES DA SILVA, *Direito Processual Penal Português. Noções e princípios gerais, sujeitos processuais, responsabilidade civil conexa com a criminal, objeto do processo.* Vol. I. Lisboa: Universidade Católica Editora. 2017. Pg. 79 e 80.; *Idem*, *Bufos, infiltrados e arrependidos. Os princípios Democrático e da Lealdade em processo penal in* Direito e Justiça, Revista da Faculdade de Direito da Universidade Católica, Vol. VIII, II, 1994. Pg. 28 e 29.

[251] GERMANO MARQUES DA SILVA, *Bufos, infiltrados e arrependidos… Op. Cit.* Pg. 31; *Idem*, "*Curso de Processo Penal… Op. Cit.* Pg. 235.

[252] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade… Op. Cit.* Pg. 854.

[253] *Ibidem*. Pg. 854.

[254] Pode ser definido como o "computador que oferece um serviço de rede que permite que os seus utilizadores estabeleçam ligações indiretas a outras redes. Assim um utilizador que se ligue a um proxy e de seguida solicite uma ligação a outro serviço (página da internet, arquivo, etc…) o proxy vai fornecer essa informação usando um IP diferente daquele que o utilizador tem na sua ligação à internet. Desta forma um servidor proxy serve de intermediário entre o utilizador e o serviço que este procura, uma vez que o conteúdo pode estar bloqueado no país onde o utilizador se encontra.". *Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 154.

[255] Corresponde a uma "rede de computadores infetados e controlados pelo seu ator através de um canal de «comando e controle». O seu ator (botmaster) controla toda a rede infetada (bots ou zombie), dando ordens e

Network)[256]. E essa dissimulação traz consigo implícita a ocultação dos respetivos autores (muito embora, como refere Armando Dias Ramos, "nem sempre os titulares das ligações da Internet possam estar direta ou indiretamente relacionados com os autores dos crimes").[257]

Ora, a identificação do autor do crime só será possível mediante uma investigação prévia em ambiente digital por parte do agente. Por regra, só assim será possível ao agente interagir, posteriormente, com o suspeito nesse meio e, por essa via, eventualmente recolher prova da prática do crime (ou da sua iminência).[258] Por conseguinte, embora seja legítimo questionar se poderá o Estado, recorrendo a esta técnica de investigação, tratar o mero suspeito como um verdadeiro inimigo, o que é facto é que o RJAE nada determina que a ação tenha que ser direcionada para um ou mais suspeitos, apenas admitindo a sua realização, como forma preventiva, bastando que hajam fortes indícios de criminalidade, dentro do catálogo de crimes nele previsto.[259]

No entanto, admitindo que a legitimidade para a prossecução de finalidades preventivas possa ser mais dúbia e carecedora de uma maior justificação, porquanto estamos perante um método de investigação que deverá ser excecional, a lei deveria estipular, de forma expressa, requisitos adicionais como a prática anterior de factos ilícitos da mesma natureza ou natureza análoga e a existência de elevados indícios da prática futura de ilícitos criminais. Por outro lado, seria igualmente crucial a distinção legal entre as investigações digitais que decorrem em canais de comunicação «abertos» das que decorrem em canais de comunicações «fechados», em função das diferentes repercussões que terão ao nível da forma de atuação do agente e na ingerência nos direitos fundamentais dos cidadãos investigados, com inevitáveis repercussões na validade da respetiva prova recolhida.[260]

Na verdade, a resposta à questão da admissibilidade das atividades do agente quer na prossecução de finalidades preventivas, quer repressivas, deverá ser dada em função do

---

manipulando esses dispositivos informáticos para cumprir as suas ordens. A informação recebida por nome é encaminhada para locais alojados na Darkweb". *Cfr. Ibidem*. Pg. 151.

[256] Respeita a uma "ligação virtual porque a informação para uma rede privada é transportada «em cima» de uma rede e é privada face à comunicação ser cifrada ponto-a-ponto, de modo a manter a confidencialidade. As VPN são efetivamente muito usadas por empresas, universidades, etc." *Cfr. Ibidem.* Pg. 152.

[257] ARMANDO DIAS RAMOS, *A prova digital… Op. Cit*. Pg. 155

[258] Também neste sentido: DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 303.

[259] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 94 e 95.

[260] Sobre esta questão, em face da importância que assume no nosso estudo, nos debruçaremos em momento autónomo ulterior (*vide*: ponto 6.7. da Parte III).

grau de lesão dos princípios constitucionais de garantia do processo penal.[261] Daí que, para o seu desencadeamento, seja também necessária a explicitação de todos os factos que lhe sejam inerentes, nomeadamente "riscos da operação, custos financeiros, riscos para os envolvidos, violações às garantias constitucionais (a exemplo do sigilo das comunicações, inviolabilidade do domicílio, intimidade etc.), assim como os crimes que possivelmente poderão ser praticados pelo agente.[262] Só desse modo se poderá cumprir um mínimo que justifique a intervenção estadual e a inerente restrição de direitos, liberdades e garantias, em ordem a uma efetiva administração da justiça penal.

Ainda no mesmo sentido, também a estipulação de forma expressa do requisito de exceção ou de *ultima ratio* na utilização das ações encobertas como meio de obtenção de prova se configuraria essencial, na medida em que, na linha do pensamento de Benjamim Rodrigues, o recurso às mesmas só se justificará apenas e somente quando "face a toda a pletora de meios (obtenção de prova), consagrados no CPP, nenhum deles se afigure apto, suficiente e adequado a permitir a aquisição de material probatório incriminatório."[263]

Cumpre também apontar que a admissibilidade da prossecução de uma ação encoberta com fins preventivos sempre poderá ser aferida através do relato que o respetivo agente venha a fazer acerca da operação. Seguimos, assim, de perto, o entendimento do Tribunal da Relação de Lisboa, patente no acórdão de 7 de julho de 1998 (aludido por Isabel Oneto), da desnecessidade da existência prévia de inquérito a decorrer para efeitos de desencadeamento de uma ação encoberta, uma vez que o controlo dessa operação, ainda que verificado num momento posterior, sempre poderá ser feito através do relato que o agente venha a juntar ao processo.[264]

Já no que respeita à competência para a iniciativa e decisão das ações encobertas vimos em momento anterior[265] que está legalmente repartida entre o magistrado do MP e o JIC, consoante ocorra no âmbito do inquérito de um processo criminal já em curso ou no âmbito de uma investigação de prevenção criminal, respetivamente. Sucede que se esta repartição de competências parece estar bem delimitada no que toca às ações encobertas

[261] SANDRA PEREIRA, *A recolha de prova… Op. Cit.* Pg. 147.
[262] MARLLON SOUZA, *Crime organizado e infiltração policial – parâmetros para a validação da prova colhida no combate às organizações criminosas.* São Paulo, Atlas, 2015, Pg. 67 a 75. *Apud Ibidem*
[263] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Novos Métodos "Científicos"… Op. Cit.* Pg.126.
[264] ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 127 e 128.
[265] *Vide*: Ponto 4.2. da Parte II.

clássicas, reguladas pelo RJAE, já nas ações encobertas digitais a Lei 109/2009 revela-se omissa.

Para além do referido, a Lei também não nos oferece resposta ao que deverá suceder à prova que tenha sido alcançada por meio de uma ação encoberta digital quando ela ainda não tinha sido devidamente autorizada. Ora, embora estejamos conscientes de que as ações encobertas constituem uma restrição de direitos fundamentais particularmente intensa e, por essa razão, uma matéria da reserva de Juiz[266], a verdade é que se trata hoje de um método de obtenção de prova essencial e que cujo sucesso exige medidas excecionais.

De facto, em ambiente digital tudo decorre de forma bastante mais rápida e instantânea do que em ambiente físico, pelo que, por vezes, a espera por uma autorização judicial para atuar poderá significar o insucesso da investigação. Neste sentido, Armando Dias Ramos alerta-nos para o facto de, com o alojamento de conteúdos na c*loud computing* (sistema de computorização que permite o armazenamento e o acesso remoto a vários conteúdos de forma infinita, acessível a partir de vários dispositivos e em vários locais), a prova digital deixa de estar alojada num só local para ficar acessível, num espaço virtual, a partir de vários dispositivos, de forma simultânea. Com essa inovação, uma prova suscetível de ser produzida em ambiente informático-digital que não seja logo recolhida, ou preservada imediatamente, pode ser apagada ou modificada pelo suspeito num ápice, mediante o acesso ao local de armazenamento na *cloud* através de um outro dispositivo.[267]

Ora, em face do exposto, as especificidades das ações encobertas digitais levam-nos, assim, a adotar uma posição menos exigente quanto à validade da prova que tenha sido obtida em momento anterior à autorização judicial habilitante. Assim, por exemplo, em casos de divulgação de imagens de abuso sexual de menores, de rapto ou escravidão de menores, quando esteja iminente a prática de crime contra a vida ou ofensa à integridade física de menores de 16 anos, atento o *periculum in mora* da intervenção da autoridade judiciária, deverá ser legitimada a realização de diligências urgentes por despacho do MP, que, nem por isso, devem deixar de ser imediatamente remetidas para a sua posterior validação pelo JIC. Concorrem para este nosso entendimento mais permissivo duas razões justificativas: primeiro, a rapidez com que os acontecimentos ocorrem em plano informático-digital, que permite a eliminação imediata de prova incriminatória[268]; segundo, o facto de a

[266] Neste sentido: DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 63.
[267] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 121 e 122.
[268] *Ibidem.* Pg. 273.

admissão de diligências urgentes nestes moldes não ser capaz de chegar a violar os ditames da Constituição da República Portuguesa, uma vez que, embora fosse preferível uma autorização prévia judicial à atuação do agente, a intervenção e validação posterior do Juiz ainda permitirá observar as imposições constitucionais.[269]

Em jeito de conclusão, a validade da prova obtida naqueles termos deverá encontrar justificação na própria natureza da própria ação encoberta digital e no facto de, de outra forma, não ser possível descobrir a verdade material e efetivar a justiça do caso concreto.

6.5. Identidade virtual: a necessidade de imposição de limites qualitativos e quantitativos

É pacífico que a atuação do agente encoberto digital ao abrigo de uma identidade fictícia constitui algo inerente às suas atividades. De facto, para além de esta ser uma prerrogativa legalmente prevista pelo RJAE, corresponde, na verdade, a uma caraterística que inerente à própria natureza das suas atividades.

No entanto, se prerrogativa atribuída pelo art. 5º do RAJE preserva toda a sua utilidade e conveniência quando em causa está a atuação do agente encoberto físico, o mesmo não poderemos afirmar quando em questão estão as atividades investigativas de um agente encoberto em espaço digital. Analisando o *modus operandi* do agente encoberto digital, facilmente se compreende que a ocultação da sua identidade é, no fundo, o procedimento normal na interação com terceiros, pelo que não constitui algo inovador num contexto em que, como sabemos, o contacto é feito essencialmente por detrás de um aparelho eletrónico e com recurso a uma identidade não real.

Assim, é de fácil perceção a desnecessidade de previsão legal do recurso à identidade fictícia, não se justificando para a concreta figura do agente encoberto virtual a aplicabilidade do art. 5º do RJAE (pelo menos nos moldes em que está escorado).[270] Isto

[269] Segundo Juliana Campos a volatilidade da prova digital e a facilidade com que a mesma pode ser adulterada ou eliminada justifica, em casos "de urgência", que métodos como estes possam ser autorizados por despacho do MP, sem prejuízo da exigência de posterior validação pelo Juiz. A aferição da legalidade da autorização posteriormente dada pelo Juiz passará pela análise dos "conhecimentos disponíveis no momento em que aquela foi dada, em vez dos que advierem em virtude da sua execução". *Cfr.* JULIANA FILIPA SOUSA CAMPOS, *O Malware… Op. Cit.* Pg. 169 e 170.

[270] Também neste sentido: ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 87. Segundo o Autor, a inaplicabilidade em concreto da *ratio legis* do art. 4º do RAJE, isto é, da necessidade de proteção que é devida ao agente encoberto ou terceiro (e, reflexivamente, da sua família) torna prescindível o recurso ao expediente e formalismo mencionado no art. 5º do RAJE.

porque, socorrendo-nos das palavras de David Silva Ramalho, "a participação em qualquer interação *online* não implica um risco acrescido para a segurança do agente que justifique o recurso à identidade fictícia, nos termos legais, uma vez que os suspeitos não têm, à partida, qualquer elemento identificativo seu. Em rigor, o mesmo nome de utilizador pode até ser usado por vários agentes. Assim, não haverá, em princípio, necessidade de criação de uma identidade fictícia, nos termos do art. 5º da Lei nº 101/2001, sem que tal prejudique a existência de uma verdadeira acção encoberta".[271]

Deste modo, atendendo à teleologia da norma, concluímos não existir, em princípio, necessidade de previsão de criação de uma identidade fictícia ou, pelo menos, nos exatos termos do artigo 5º da Lei nº 101/2001, a não ser que o agente encoberto digital venha a prestar, posteriormente, depoimento relativamente aos factos que apurou, caso em que poderá testemunhar ao abrigo das normas previstas na Lei nº 93/99, de modo a garantir a sua plena segurança.[272]

Por outro lado, a Lei não se revela suficientemente esclarecedora quanto ao que se deverá entender por "identidade fictícia". De facto, a criação de um nome fictício não será exatamente o mesmo que a criação de uma identidade fictícia, não sendo possível a extração do seu significado a partir da letra da Lei. Neste sentido, Armando Dias Ramos evidencia que a utilização pelo agente encoberto digital de *nicknames* ou alcunhas em perfis da Internet ou no meio em que imiscui não corresponde à utilização de uma identidade, na verdadeira aceção do termo.[273]

Em face do exposto, David Silva Ramalho questiona se a criação de um perfil falso com dados que tornam a pessoa identificável, por exemplo, um perfil no Facebook, a criação de um *username* para interagir com terceiros que se identificam do mesmo modo ou até mesmo a utilização do *username* de um terceiro, previamente integrado no meio onde o agente se quer infiltrar, estarão dentro do conceito de "identidade fictícia" e, por essa via, sujeitas ao regime previsto no art. 3º do RJAE.[274] Entre nós, reconhecendo as dificuldades que o preceito convoca, parece-nos que seria importante especificar os termos e a extensão da putativa atribuição da "identidade fictícia".

---

[271] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 305.
[272] *Ibidem*. Pg. 305.
[273] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit*. Pg. 87.
[274] *Ibidem*. Pg. 304.

Ademais, se é verdade que o conceito de "identidade fictícia" reveste particular importância e assume pleno sentido quando em causa está uma ação encoberta clássica, na medida em que, ao contrário do que sucede nas ações encobertas digitais, não basta o mero uso de um nome fictício, nas ações encobertas digitais a questão perde relevância. De facto, o agente encoberto físico necessita de munir-se de uma aparência mais exigente, nomeadamente através da criação de uma imagem física suficientemente credível e retratadora de uma determinada personalidade, da posse e utilização de documentos falsos, da interação com novas pessoas, preferencialmente pertencentes ao núcleo social onde se centram as investigações, da criação de redes sociais, entre outras. Já o agente encoberto digital bastar-se-á, em princípio, com a criação de um *username* ou *nickname* que lhe permita manter o seu anonimato e contactar à distância com os potenciais criminosos.[275]

De outro ponto de vista, uma outra questão que também não poderá ser desvalorizada prende-se exatamente com os limites à criação de identidades fictícias virtuais. Na linha do pensamento de Armando Dias Ramos, impõe-se como extremamente necessário o balizamento do número e qualidade de identidades virtuais permitidas: do número, porque não deverá ser de admitir a possibilidade de o agente se servir para uma única ação encoberta de inúmeras identidades fictícias[276]; da qualidade porque a própria identidade fictícia que a ser-lhe atribuída deverá ser idónea ao resultado que pretende com ela alcançar. A utilização de nomes excessivamente sugestivos ou pouco adequados para o contexto de investigação, assim como a utilização de uma "imagem" virtual pouco plausível, poderão constituir motivo suficiente para determinar o insucesso da ação encoberta. De maneira que, como bem evidencia F. Bueno de Mata, a previsão legal de criação de um *nickname* suficientemente credível, capaz de soar familiar a terceiros eventualmente relacionados com a prática de crimes cibernéticos, com quem procure estabelecer laços e conquistar a sua

[275] No mesmo sentido, DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Ci*t. Pg. 198.

[276] O que não obsta a que as atividades do agente encoberto digital possam ser desenvolvidas por diversos agentes sempre que não se verifique a necessidade de ser concretizado um contacto pessoal entre o agente e o(s) suspeito(s) investigados. Para tanto, basta, como já advogámos anteriormente, que os vários agentes atuem em consonância, através de um guião no qual venha descrita toda a atividade e forma de interação, de modo a evitar criar uma suspeita de que interagem com o(s) suspeito(s) pessoas diferentes. Obviamente que tal não poderá suceder quando o agente tenha que encetar comunicações, sobretudo por videochamada, em que se exige a continuidade do mesmo agente (ou terceiro). *Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 87.

confiança, seria, de todo, conveniente. De facto, um *nickname* apelativo pode ser um ótimo ponto de partida para dar início a uma conversa por via da Internet.[277]

De notar que, como refere David Silva Ramalho, a estipulação de um "limite numérico à criação de *usernames*" com a obrigatoriedade da "sua comunicação em momento prévio à respectiva utilização", acaba também por se revelar fundamental para evitar situações indesejáveis de frustração dos limites subjacentes à investigação. Pense-se, a título de exemplo, no facto de permitir evitar que o agente crie, de forma autónoma, contas para, posteriormente, as utilizar com o intuito de provocar o suspeito e depois apenas fazer constar dos autos a interação ocorrida através de uma conta da qual consta apenas o resultado final da provocação.[278]

Acresce ainda o facto de todas as circunstâncias relacionadas com a identidade fictícia deverem constar devidamente do relato do agente: a ser admitida a utilização de mais do que uma identidade fictícia no âmbito de uma mesma ação encoberta, se uma determinada prova foi produzida em resultado da sua atuação com a identidade fictícia X, deverá isso ser registado; se foi produzida através da sua atuação com a identidade fictícia Y o mesmo deverá suceder. Além disso, a utilização de uma determinada identidade fictícia deverá ser comunicada à autoridade judiciária em momento anterior à investigação.[279] Note-se que não podemos perder de vista a exigência de uma ação encoberta controlada, desenvolvida dentro dos parâmetros previstos na autorização da autoridade judiciária e cumpridora dos princípios da legalidade, da necessidade e da proporcionalidade.

6.6. A fundada e necessária anexação do relato do agente ao processo

Dúvida pertinente, e que não poderá escapar das nossas considerações, prende-se também com a extensão da previsão, no âmbito das ações encobertas digitais, do princípio-regra da não anexação do relato do agente encoberto digital ao processo, tal como se encontra pensado para as ações encobertas clássicas.

De facto, se a aplicabilidade de um tal princípio no âmbito das ações encobertas físicas se pode perfeitamente ancorar no argumento da necessidade de garantir a proteção e

[277] FEDERICO BUENO DE MATA, *El agente encubierto en Internet… Op. Cit.* Pg. 303.
[278] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 306.
[279] Também neste sentido, DAVID SILVA RAMALHO, *Métodos ocultos... Op. Cit*. Pg. 306.

segurança pessoal do agente, já no âmbito de uma atividade investigativa, em ambiente virtual, é algo que se pode questionar.

Como já se evidenciou em momento anterior[280], os riscos que um agente encoberto digital assume – na sua pessoa e no seu círculo pessoal – não são equiparáveis aos de um agente encoberto físico. Efetivamente, a atividade investigativa informático-digital decorre num ambiente pouco provável de ter consequências atentórias à segurança pessoal de quem a ela se dedica, na medida em que tudo basicamente acontece por detrás de um aparelho eletrónico e, mesmo na hipótese de a operação falhar, os suspeitos investigados nunca terem sequer acesso a uma imagem ou qualquer informação que o possa associar à investigação. Assim, é indubitável que o mundo da investigação digital beneficia da vantagem de permitir uma autêntica investigação oculta, uma infiltração *"*puramente virtual e impessoal".[281]

Em face disto, a consagração do princípio-regra da junção do relato do agente apenas nos casos da sua indispensabilidade probatória, escorada no argumento da necessidade de garantir a segurança pessoal do agente, perde completamente o seu sentido no âmbito das ações encobertas digitais. Só em casos muito excecionais – como, por exemplo, na remota situação em que escape alguma informação sobre a identidade do agente e que o possa, com alguma probabilidade associar às atividades investigativas e, por essa via, o colocar efetivamente em risco – é que uma tal regra-excecional se justificaria.[282]

Note-se que, com isto, não pretendemos afirmar que o agente encoberto digital não corre riscos na sua segurança pessoal. De facto, tal como evidenciam Stangherlin e Petean, ainda que o agente virtual não sofra iguais ameaças e perigos físicos inerentes à infiltração presencial, deverá continuar a preservar-se o dever de o proteger na sua intimidade e privacidade, principalmente diante da natureza de certos crimes investigados. Por outro lado, não pode ser descartado o facto de a estas investigações em ambiente digital estar também associado um risco de "contaminação psíquica, de criação de desequilíbrio emocional e moral, até mesmo o surgimento de uma crise de identidade pessoal", em face do nível de

[280] *Vide:* ponto 2.2. da Parte I.
[281] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 308.
[282] Contra este entendimento se parece posicionar Duarte Rodrigues Nunes, de acordo com o qual "no caso do agente infiltrado online, ainda que não se coloque a questão da possibilidade de voltar a utilizar aquela pessoa noutras ações encobertas (podendo sempre utilizar um outro nickname, ainda que podendo ser necessário criar uma nova "pegada digital"), continuará a, tal como nas ações encobertas "clássicas", colocar-se a questão da proteção da vida e da integridade física do agente infiltrado e dos seus familiares", *Cfr.* DUARTE RODRIGUES NUNES, *O agente infiltrado online… Op. Cit.* Pg. 79.

envolvimento que estas ações exigem.[283] Para além destes perigos, também o sucesso da ação que, por regra, decorre por longos e largos meses, depende fortemente das caraterísticas pessoais do agente. Assim, o nervosismo, a falta de traquejo e a incapacidade para lidar psicologicamente com o mundo virtual poderão obstar ao êxito das atividades investigativas.[284] Todos estes factos exigem um especial cuidado com a pessoa do agente. Porém, o que não se pode negar é que mesmo pensado em todos esses riscos, as ameaças que lhe estão inerentes não são equiparáveis àquelas que em ambiente físico se fazem sentir, do que resulta a desrazoabilidade de a não anexação do relato do agente ao processo ser escorada (pelo menos apenas) naquele argumento de proteção do agente.

Por outro lado, concorre ainda para a necessidade de anexação do relato do agente ao processo os riscos que decorrem da natureza da prova produzida em ambiente digital. Se a fragilidade da prova obtida pelo agente encoberto físico (em função da própria natureza do método de obtenção de prova) é uma realidade incontestável, em ambiente digital essa vulnerabilidade torna-se ainda mais evidente. Sendo o agente digital dotado de ferramentas técnicas altamente inovadoras que lhe permitem ter acesso a milhares de informações restritas e confidenciais, só um relatório detalhado, onde constem os procedimentos forenses utilizados para a sua recolha, poderá demonstrar a legitimidade da prova que tenha sido por si recolhida.

Efetivamente, a prova digital apresenta caraterísticas peculiares, inexistindo qualquer paralelo de comparação com as provas físicas: é fragmentária, dispersa, alterável, apagável, manipulável, invisível e espacialmente dispersa.[285] E é essa volatilidade e fragilidade com que se apresenta que acabam por impor, de forma particularmente exigente, o cumprimento de certos requisitos de verificação de fidedignidade e de garantia da cadeia de custódia (e que, por regra, não são exigidos relativamente à prova recolhida pelos agentes encobertos clássicos).[286]

---

[283] MARINA STANGHERLIN, FABIANO AUGUSTO PETEAN, *Agente Infiltrado… Op. Cit*. Pg. 54. Também sobre a pressão psicológica a que o agente encoberto fica sujeito nas suas atividades: ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 86 a 88.

[284] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 73

[285] *Ibidem.* Pg. 119. Também neste sentido: SÓNIA FIGALDO, *A utilização de inteligência artificial… Op. Cit.* Pg. 134.

[286] DAVID SILVA RAMALHO, *O uso de malware… Op. Cit.* Pg. 235; *Idem, Métodos ocultos… Op. Cit.* Pg. 106.

Do que resulta, assim, nas palavras de David Silva Ramalho, que "o reduzido risco para a segurança do agente, aliado à fragilidade da prova (…) tornam, por um lado, objectivamente indispensável que o relato seja junto aos autos e, por outro, tornam injustificável a sua não junção"[287]. Não há, pois, razões capazes de justificar o afastamento das garantias de defesa e do direito do sujeito investigado ao contraditório, direito constitucionalmente reconhecido pela nossa Lei Fundamental no seu art. 32º, nºs 1 e 5.

Sob outra perspetiva, questão igualmente ponderosa destacada por alguns Autores como Fátima Mata-Mouros[288], tem sido também a de saber se o relato do agente encoberto deverá conter a descrição de toda a sua atuação. No que a essa questão respeita, David Silva Ramalho, prosseguindo no sentido de uma resposta positiva, aponta que, se a ação encoberta se desenrolar pelo período de um ano, não é razoável que apenas o relato apenas seja entregue no seu final e que contenha acontecimentos realizados num lapso de tempo tão extenso, sem qualquer controle judiciário. Assim, no seu entender, a não violação das normas do art. 18º, nº 2, 32º, nº 6 e 272º, nº 2 e 3 da CRP implica que o agente encoberto realize relatórios, no mínimo de 15 em 15 dias (ou, no limite, de 30 em 30 dias), onde condense elementos que tenham sido gradualmente recolhidos, de modo a efetivar a sindicação das suas atividades investigativas.[289] Note-se que este controlo das atividades investigativas é já uma realidade no ordenamento jurídico brasileiro, na medida em que o art. 190º-A § 1º da Lei 13.441/17 prevê expressamente a possibilidade da autoridade judicial e do Ministério Público requisitarem relatórios parciais da operação de infiltração digital antes do término do prazo estipulado para o período de investigação (que não poderá ser superior a 90 dias no âmbito da criminalidade grave), o que permite assegurar que as ações encobertas digitais decorram com estrito respeito pelas regras e princípios que lhes estão subjacentes.

Deste modo, acompanhando o autor anterior, consideramos que o relato que venha a ser anexado ao processo, capaz de evidenciar os traços gerais da ação do agente, deverá, assim, ser complementado por um conjunto de registos efetuados pelo mesmo, onde venham descritos determinados pormenores que remontem a específicos momentos da investigação.

---

[287] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 308.
[288] *Vide*: FÁTIMA MATA-MOUROS, *Infiltrados fora da lei, Sub Judice – justiça e sociedade*, Coimbra, nº 18, 2000. Pg. 61 e ss.
[289] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 42 e 43.

Para além disso, tal como defende Armando Dias Ramos, a ação encoberta deverá ser controlada pelo JIC com uma periodicidade de, no limite, 30 dias, de modo a evitar a transgressão de direitos inalienáveis dos visados na investigação e a sobressair a transparência da investigação criminal. [290]

A necessidade de registos periódicos, onde constem descritos determinados pormenores da investigação impõe-se por variadíssimas razões. Pense-se, por exemplo, na natureza das comunicações. Como sabemos, numa ação encoberta clássica, o contacto entre o agente e os suspeitos investigados faz-se, geralmente, através de uma única comunicação, cara-a-cara ou por telefone, naturalmente circunscrita no tempo. Já no ciberespaço a comunicação poderá processar-se de formas variadas, podendo a própria contagem do número de contactos tornar-se muito mais difícil de apurar. No cenário de um agente que começa por contactar por correio eletrónico com um determinado sujeito e que, entretanto, ganha a sua confiança e consegue obter o seu *Whatsapp*, onde vai obter mais informações detalhadas sobre a eventual prática de um crime, poderá implicar que se considere ter existido não apenas um único contacto, mas vários contactos. A aferição do número de contactos poderá ser feita considerando, desde logo, o tempo de conversa entre as partes. Se as transmissões são feitas rapidamente, por exemplo, num único dia, é mais provável que constituam uma conversa única; por outro lado, deverá ainda ser considerado o número de transmissões, na medida em que é mais provável que uma transmissão, traduzida numa única pergunta à qual se segue uma resposta, seja encarada como um único contato; deverá ainda ter-se em consideração o número de interrupções e transições de assunto nas conversas, bem como o meio através do qual as comunicações são trocadas. Por exemplo, as conversas ocorridas em salas de *chat* decorrem "em tempo real", pelo que têm início, meio e fim. O que mesmo já não acontece com as comunicações que são feitas por correio eletrónico.[291]

De relevar que o registo de número de contactos não se revela despiciendo. Na verdade, permite, desde logo, o controlo da própria ação encoberta e a averiguação do respeito pelos seus limites. Por outro lado, o registo das suas atividades também assume importância para distinguir a prova que seja o resultado da sua atividade *online* durante o período de serviço da prova que tenha sido recolhida através das investigações levadas a cabo durante o período de tempo pessoal. De facto, sendo este último tipo de prova alvo de

[290] *Ibidem*. Pg. 257.
[291] DEPARTMENT OF JUSTICE, *Online Investigative Principles… Op. Cit.* Pg. 37 a 39. Disponível em: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf [Acesso em: 16 de dez. de 2021].

bastantes controvérsias, do ponto de vista da sua validade e utilidade para o processo, a especificação da sua forma e momento de obtenção no relato do agente é essencial.

Note-se que o uso de recursos o*nline* por parte de agentes fora do horário laboral para fins investigativos levanta questões conflituantes: por um lado, permite o avanço das investigações, trazendo vantagens ao nível da economia processual; por outro, poderá significar a produção de prova na ausência de controlo judicial superior. Ora, o alcance do equilíbrio entre estes interesses divergentes poderá ser feito mediante a admissibilidade da prova que seja produzida nesses termos, embora sujeita a determinadas regras e princípios. Neste sentido, entendemos que se atividades o*nline* do agente, mesmo que desenvolvidas durante o seu período de tempo pessoal, contidas dentro do escopo de uma investigação já em andamento ou realizadas com o propósito de desencadear pistas investigativas ou, simplesmente, para permitirem o aprimoramento das habilidades e conhecimentos informáticos do agente, deverão ser permitidas e valoradas no âmbito do processo. No entanto, nesse caso, o agente sempre deverá ficar sujeito às mesmas restrições e regras que sempre se lhe exigiriam na sua conduta investigativa se estivesse em serviço e a forma (e momento) de obtenção da prova deverá constar detalhadamente do seu relato.[292]

Cumpre acentuar que, nas investigações levadas a cabo pelo agente encoberto físico, o agente não pode, fora do serviço e por iniciativa própria, vigiar a casa de um suspeito investigado, mas pode perfeitamente aproveitar para ler e obter mais conhecimentos sobre estratégias de vigilância. Da mesma forma, nas ações encobertas digitais não vemos razão para criar obstáculos a esse tipo investigação – até pela facilidade processual e segurança que lhe está associada - desde que seja levada a cabo dentro daquilo que é exigido pelo princípio da proporcionalidade e de acordo com o escopo e limites da própria investigação.

Pelo exposto, estamos em condições de afirmar que são todas estas questões tão próprias do ambiente digital que, não tendo expressão no mundo físico, acabam por "implica[r] um dever acrescido de controlo por parte da autoridade judiciária e uma obrigação de registo permanente de toda a actividade empreendida pelo agente no decurso da acção".[293]

[292] *Ibidem*. Pg. 59. [Acesso em: 16 de dez. de 2021].
[293] DAVID SILVA RAMALHO, *Métodos Ocultos… Op. Cit.* Pg. 286.

6.7. A atuação do agente em canais «abertos» de comunicação *versus* em canais «fechados» de comunicação

Ao longo da presente dissertação fomos fazendo referência aos canais «abertos» e «fechados» de comunicação, tendo já sido avançado que o facto de as investigações decorrerem num ou noutro tipo de canal de comunicação acaba por determinar especificidades diferentes ao nível do grau de penetração do agente no cerne criminoso e a necessidade de as suas atividades estarem ou não dependentes da obtenção de uma prévia autorização judicial, sendo este o momento oportuno para o explanar.[294]

A distinção entre canais «abertos» e «fechados» de comunicação não constitui, na verdade, uma novidade jurídica. De facto, o ordenamento jurídico espanhol, na LECrim, aprovada pelo Real Decreto de 14 de setembro de 1882, delimita de forma sagaz, no nº 6 do

[294] Verdadeiramente paradigmático no âmbito da problemática das ações encobertas digitais e com relevo na questão que neste ponto nos debruçamos, se assumiu o recente caso, com origem espanhola, de Pedro Jésus, que foi a decisão do Tribunal Supremo, na Sala de lo Penal, a 11 de abril de 2018. Em causa esteve a alegada prática de crimes sexuais por Pedro Jésus contra as suas filhas gémeas Milagrosa e Silvia, menores, de 4 anos de idade, com o objetivo de produzir e partilhar em canais «fechados» da Internet conteúdo pedopornográfico. Em face dos crimes cometidos, previstos e punidos pelo art. 183, aps. 1,3 e 4 a), art. 192.2, art. 74.1, art. 189.1.a), art. 189.3 a) e art. 192.2 do Código Penal espanhol, Pedro Jesús foi condenado a 22 de junho de 2015, a 12 anos de prisão, ficando ainda impedido do exercício das suas responsabilidades parentais, bem como foi proibido de se aproximar e manter qualquer contacto com as suas filhas Silvia e Milagrosa, com o seu filho Teofilo e com a mãe dos seus filhos, sua esposa, pelo período de 15 anos. Para além disso, foi ainda sujeito a 10 anos de liberdade vigiada, em conformidade com o disposto no art. 192º/11 do Código Penal espanhol e perdeu a custódia parental dos seus filhos, nos termos do art. 192º/3 do mesmo Diploma. Ora, foi em sede de recurso da douta decisão que o condenado veio a invocar, entre muitos outros argumentos, que a polícia de Nova Zelândia se havia infiltrado no canal «fechado» de comunicação, meio criminoso onde tudo se passava, sem que para isso estivesse munida de uma prévia autorização judicial, em violação das regras processuais em matéria de obtenção de prova. Em face disso, apontou o Tribunal que a necessidade de uma prévia autorização judicial para toda e qualquer forma de investigação é coisa que não é pacífica, nem na doutrina nem junto da jurisprudência, mostrando o direito comparado modalidades de regulação muito diversas desta questão. Assim, refere o Acórdão que doutrinalmente há quem diferencie as meras patrulhas cibernéticas, em que tipicamente o agente investiga em canais de comunicação «abertos», acessíveis ao público em geral, das investigações que decorrem em canais «fechados», de acesso restrito, entendendo-se que só estas últimas carecem verdadeiramente de uma autorização judicial habilitante. Nesse sentido, partindo daquela destrinça, as investigações levadas a cabo em relação a Pedro poderiam, à primeira vista, encaixar-se no espetro do segundo grupo de casos. Porém, não foi isso que foi considerado nem relevado na decisão, uma vez que entendeu o Tribunal que o que esteve em causa não foi uma infiltração policial na rede através da utilização pelos agentes de polícia de uma identidade virtual fictícia, mas o uso do canal criado pelo próprio investigado pelas forças policiais, fazendo-se passar pelo criminoso através da utilização do seu *nickname*, não tendo concluído pela invalidade da prova produzida nesses moldes. Não obstante, a decisão aqui em análise releva-se pertinente, na medida em que nela se suscitou e se abriu espaço à discussão quanto à necessidade de habilitação judicial para a prática de todo e qualquer ato do agente no âmbito das ações encobertas digitais e à possibilidade de ser valorada prova que, embora produzida sem prévia autorização judicial habilitante, se revelou imprescindível à descoberta da verdade material e à realização da justiça do caso concreto.
Disponível em: https://www.poderjudicial.es/search/documento/TS/8370270/abusos%20sexuales/20180504 [Acesso em: 11 de janeiro de 2022].

seu art. 282º, o campo de atuação do agente encoberto virtual, o que o faz mediante a introdução desta diferenciação. Embora a distinção tenha sido já avançada em momento anterior[295], importa recordá-la para a melhor compreendermos.

Estando em causa uma comunicação mantida num canal dito «aberto», vulgo conhecido como um *chat, blog* ou *website* de acesso público, o seu acesso pode ser feito por qualquer cidadão comum, não carecendo de particulares exigências, estando pois na disponibilidade de qualquer um, inclusive, dos responsáveis por uma investigação criminal. O acesso é possível mediante um simples "*click*" de um *link* ou até mesmo mediante a criação de uma conta ou de um perfil, com o objetivo de observar o que naqueles sítios da Internet se passa, como conversas particulares ou públicas, ou até mesmo, eventualmente, a prática de crimes informático-digitais, sem que haja uma envolvência direta do observador.

Diferentemente, quando em causa está o acesso a um canal «fechado» de comunicação, isto é, de acesso restrito e não acessível ao público em geral, a penetração no seu núcleo dependerá, em grande medida, da conquista da confiança de quem nele participa e, portanto, de uma maior envolvência por parte de quem nele pretende integrar. Estes canais são, muitas vezes, utilizados como meio de prática de crimes informático-digitais, daí encerrarem maiores dificuldades de ingresso.

Ora, em face das diferenças que estes tipos de canais apresentam ao nível da facilidade no seu acesso, poderá apelar-se à seguinte distinção: estando em causa uma atuação mantida num canal «aberto» de comunicação, sendo o seu acesso fácil e extensível a qualquer pessoa (inclusive aos agentes), não havendo, por consequência, a necessidade de conquista de confiança dos seus utilizadores nem uma intromissão expressiva por parte do agente no eventual ilícito, estaríamos no domínio das ações encobertas; se, pelo contrário, a ação se desenvolve num canal «fechado», encerrando acrescidas dificuldades de acesso e, havendo, naturalmente, a necessidade de uma maior envolvência no cerne criminoso, já estaríamos, então, no domínio de uma verdadeira ação infiltrada. De relevar que adepta desta destrinça se manifesta a doutrina maioritária espanhola, embora o faça recorrendo a uma conceitualização diversa: o que entre nós se vem denominando por "ação encoberta", o país vizinho apelida de "ação infiltrada de curta duração", e o que entre nós se vem designando de "ação infiltrada", a doutrina espanhola denomina como "ação encoberta". Veremos,

[295] *Vide:* Ponto 2.1. da Parte I.

porém, que o espírito da distinção é, na verdade, o mesmo, apenas diferindo a denominação atribuída.

Ora, por "ação infiltrada de curta duração" entende a doutrina espanhola ser aquela "que o agente leva a cabo, no âmbito digital, sempre que limitada à ocultação da condição de policial e ao recurso a falsidades que, por mínimas ou de pouca significância, não são capazes, por si só, de gerar uma confiança no interlocutor investigado".[296] No prisma oposto, estaremos já no âmbito de uma "ação encoberta" sempre que a atuação do agente vá além da criação de um *nickname,* com a criação de algo muito mais complexo, como uma personagem, e em que o engano surge como fonte de vício do consentimento do cidadão investigado, gerando uma confiança artificial entre a pessoa do agente e a do investigado que, a não existir, impossibilitaria a comunicação.[297] Tem-se, pois, que a diferença opera ao nível do grau de ingerência do agente no ilícito e das respetivas repercussões no núcleo dos direitos, liberdades e garantias dos suspeitos investigados. De maneira que o nível de engano com que o agente prossegue, a forma como é capaz de viciar a perceção e alcançar o consentimento dos investigados configuram-se essenciais na determinação do nível de infiltração e na necessidade de a ação obedecer a determinados requisitos legais mais exigentes.

Deste modo, segundo aquela doutrina, as operações digitais enquadráveis no âmbito da prevenção criminal, que não se prolonguem no tempo e que não exijam contactos intensos com os investigados capazes de alcançar a sua confiança, à partida, não necessitam de estar sujeitas aos rigorosos trâmites legais que estão previstos para o "agente encubierto".[298]

---

[296] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit*. Pg. 263.
[297] *Ibidem*. Pg. 264.
[298] Javier Zaragoza Tejada, inserindo-se nessa doutrina, invoca um caso espanhol de pornografia infantil, vertido na sentença do Supremo Tribunal nº 767/2007 de 3 de outubro, destacando a conveniência de, em certo tipo de investigações criminais com finalidades preventivas, ser permitida uma atuação policial prévia ao desencadeamento da ação encoberta propriamente dita. Note-se que, por vezes, tais atuações, traduzidas, por exemplo, no simples acesso a *sites* de cariz público (sem estabelecer contactos de relevo com os suspeitos investigados), permitem, como sucedeu no caso, reunir um conjunto de indícios suficiente e plausível para, posteriormente, justificar e dar aso a uma ação encoberta. Em causa esteve o registo e infiltração de um agente da Guardia Civil, com o *nickname* "rata", num *site* de acesso público, um dito canal «aberto» de comunicação, suspeito *locus delicti* da troca de conteúdo pedopornográfico, com o intuito de observar o que nele se passava, sem que ainda estivesse munido de uma prévia autorização judicial. Tratou-se, assim, de uma espécie de "medida cautelar de polícia", capaz de reunir indícios suficientes da existência de uma verdadeira rede, que justificasse o desenvolvimento de uma ação encoberta formal, depois que obtida a respetiva autorização judicial por parte do JIC. Vide: https://vlex.es/vid/facilitacion-pornografia-infantil-p-31969904 [Acesso em: 18 de maio de 2022]. *Apud* JAVIER ZARAGOZA TEJADA, *El Agente Encubierto "online in* Investigación tecnológica y derechos fundamentales: comentarios a las modificaciones introducidas por la ley 13/2015, ARANZADI / CIVITAS, 2017. Pg. 335 a 339.

Pellucci considera que estaremos numa dessas situações sempre que, por exemplo, um agente, navegando num canal «aberto» de comunicação, aceite receber ficheiros digitais com conteúdos ilícitos (*v.g.* de pornografia infantil), fornecidos livremente pelos criminosos através de um *chat* ou de um fórum de acesso público. Na sua ótica, estes casos não assumem relevo penal, na medida em que "não há uma infiltração propriamente dita, mas um acesso disfarçado que pode levar ou não a alguma situação penalmente relevante", existindo uma vontade prévia na prática do ilícito que sempre se concretizaria, quer os conteúdos fossem recebidos pelo agente ou por qualquer outra pessoa (bastando, portanto, a existência de um qualquer destinatário); ademais, o consentimento na conversa é tácito e o engano é mínimo, não sendo capaz de criar nos investigados qualquer intenção criminosa ou de ferir gravemente princípios constitucionais[299], do que resulta a admissibilidade da prova produzida naqueles moldes.[300]

Ora, embora seja legítimo questionar a admissibilidade da mera criação pelo agente de um *nickname,* do seu cadastro em *sites,* fóruns ou *chats* de acesso público, relacionados com a prática de crimes, com o objetivo de patrulhar conversas alheias e, por essa via, descobrir eventuais ilícitos criminosos, sem que para isso esteja munido de uma prévia autorização judicial, a verdade é que, ao contrário do que sucede em contexto físico, em ambiente digital o anonimato e o recurso a *nicknames* e *usernames* constituem a regra.[301]

---

[299] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit*. Pg. 264.

[300] Veja-se, neste sentido, a decisão proferida pelo Tribunal do Ohio, no caso *United States v. Charbonneau,* em que contra o argumento da inadmissibilidade da valoração como prova das declarações feitas em salas de c*hat* e do *e-mail* com ficheiros de pornografia infantil enviado por Charbonneau, por violar graves princípios e direitos constitucionais do arguido, entendeu o Tribunal que as declarações não se encontravam abrangidas no núcleo essencial do seu direito à privacidade, uma vez que a participação em salas de c*hat* é estendível a qualquer pessoa, inclusivamente a agentes encobertos, podendo nesse meio recolher informações eventualmente incriminatórias, tal como sucede com conversas em locais em públicos ("*todas as evidências coletadas pelo FBI nas salas de bate-papo resultaram da presença de agentes disfarçados nas salas. Claramente, quando o Réu se envolveu em conversas em salas de bate-papo, ele correu o risco de falar com um agente disfarçado. Além disso, o Réu não poderia ter uma expectativa razoável de privacidade nas salas de bate-papo.").* Disponível em: https://law.justia.com/cases/federal/district-courts/FSupp/979/1177/1446971/ [Acesso em: 01 de abril 2022]. *Apud* DAVID SILVA RAMALHO, *Métodos Ocultos… Op. Cit.* Pg. 282 e 283; Também com interesse prático nesta matéria se assumiu a STS 752/2010 de 14 de julho, em que perante a suscitação da violação do direito ao sigilo das comunicações, se considerou que a disponibilização de dados meramente identificativos com a captação de mensagens e contactos efetuados através da Internet não constitui uma atividade propriamente lesiva dos direitos, liberdades e garantias do suspeito investigado, na exata medida em que o acesso a essas informações, sendo públicas, estão na livre disponibilidade de qualquer usuário da Internet, não havendo, portanto, necessidade de qualquer autorização judicial prévia para a sua obtenção (se um qualquer cidadão comum poderá a elas ter acesso, por maioria de razão, os OPC também poderão). Disponível em: https://vlex.es/vid/-218422135 [Último acesso em: 04 de março de 2022].

[301] MARINA STANGHERLIN, FABIANO AUGUSTO PETEAN, *Agente Infiltrado… Op. Cit.* Pg. 35.

Tal não configura um engano propriamente dito, nem um facto que careça de particulares exigências legais, partindo do pressuposto que "pequenas mentiras são inerentes ao mundo virtual em que o agente se move".[302] Note-se que todos aqueles que fazem uso da Internet sabem que estão perante um mundo fictício, em que a maioria das vezes aqueles com quem contactam não se apresentam com os seus dados reais. E essa é uma realidade que se estende a todos os que navegam na *Web* - inclusive aos agentes do Estado -, não constituindo um facto juridicamente relevante.

Como elucida Pellucci, o simples acesso aos ditos canais «abertos» de comunicação é algo que é livre e inerente à atividade policial, na medida em que "se qualquer cidadão pode fazê-lo sem restrições e de forma anónima, mesmo que necessário o registo prévio, não existe lógica em negar tal prática a um agente do estado."[303] Esta pesquisa de informação em redes abertas, também designada por OSINT (*Open Source Intelligence),* está, pois, na livre disponibilidade dos OPC. Assim, as provas obtidas com recurso a estas fontes abertas, entendidas como aquelas que se encontram acessíveis a qualquer pessoa e que podem ser consultadas inúmeras vezes, são insuscetíveis de lesar qualquer direito fundamental dos cidadãos investigados, na medida em que para elas aceder não se revela necessária qualquer intromissão e violação de acessos condicionados.[304]

Assim, entre nós, em face do exposto, na linha do pensamento de Armando Dias Ramos, consideramos que as informações que possam ser obtidas através de canais «abertos» de comunicação, não exigindo quaisquer medidas excecionais de investigação, como a utilização do agente encoberto, não deverão estar necessariamente sujeitas aos termos definidos no RJAE. Tais ações de investigação em canais «abertos» de comunicação deverão antes ser reconduzidas a medidas cautelares de polícia (previstas no art. 249º do CPP) que, embora correspondendo ao exercício de uma competência geral de investigação criminal[305], constituem uma prévia e necessária medida investigativa às ações encobertas. Efetivamente, não vemos razão aparente para negar uma tal prática entre os OPC que venham, posteriormente, a encetar ações encobertas digitais.

---

[302] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.*. Pg. 265.
[303] *Ibidem*. Pg. 255. Também neste sentido prosseguiu um grupo de investigadores dos Estados Unidos da América, *vide:* DEPARTMENT OF JUSTICE, *Online Investigative Principles… Op. Cit.* Pg. 10. Disponível em: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf [Acesso em: 14 de dez. de 2021].
[304] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 164.
[305] *Ibidem*. Pg. 164.

Deste modo, só nos casos em que depois de investigar preventivamente, ao abrigo daquela medida cautelar de polícia, o *site* de acesso público e de recolher indícios suficientes de uma prática criminosa, o agente pretender intervir de forma ativa no ilícito, procurando iniciar uma conversa com os suspeitos investigados ou praticar qualquer ato de maior relevo, é que a autorização judicial para atuar, ao abrigo do RJAE, se revela imprescindível, não propriamente pela necessidade de criação de uma identidade fictícia, mas pela futura interação enganosa e dissimulada que com ela se pretenderá promover com os suspeitos.[306]

Concretizando, estando em causa uma operação que decorre num dito canal de comunicação «fechado», faz todo o sentido que a atuação do investigador esteja dependente de uma prévia autorização e seja ladeada de requisitos mais rigorosos, atendendo ao meio em que se desenvolve. De facto, estes grupos, em que o anonimato dos seus integrantes permite o fomento da atividade criminosa, encerram uma maior dificuldade para a investigação criminal, por se dotarem de uma maior segurança informática e de o ingresso de novos utilizadores estar dependente da conquista da confiança dos seus pretéritos utilizadores, o que exige um maior envolvimento do agente no seio criminoso, com a eventual prática de atos ilícitos como seja o envio de conteúdo ilícito. [307] Mas se, ao invés, em causa estiver uma comunicação mantida num canal «aberto», de acesso fácil e público, não carecedora de um grau de infiltração de relevo nem da prática de atos capazes de permitir a conquista da confiança dos investigados, entendemos que a autorização para atuar e a sua obediência aos requisitos legais ínsitos no RJAE ainda não se revela necessária.[308]

Efetivamente, a patrulha em canais «abertos», no âmbito da prevenção criminal, não implicando um engano propriamente dito por parte dos OPC relativamente aos suspeitos observados (no sentido de conseguir penetrar no seu meio e ter acesso a eventual prova incriminatória), não comporta uma particular lesão dos seus direitos, liberdades e

---

[306] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 259.

[307] MIGUEL ÁNGEL LORCA SÁNCHEZ, *El derecho al secreto de las comunicaciones. Influencia de la jurisprudencia y análisis de su aplicación en la práctica jurídica.* Tesis Doctoral. Universitat d' Alacant, Facultad de Derecho, Departamento Derecho Mercantil y Derecho Procesal. Enero 2021. Pg. 144.

[308] Do mesmo modo prossegue FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit*. Pg. 252 e 253; Armando Dias Ramos, apresentando um idêntico pensamento, discorda da posição defendida por Duarte Nunes, quando o Autor afirma que "a conduta do agente encoberto poderá consistir no "patrulhamento" de sítios da Internet, chats ou newgroups abertos ou acedidos com o consentimento de um dos participantes", entendendo que o facto de um agente "patrulhar" um sítio da Internet não determina automaticamente que se esteja perante uma verdadeira ação encoberta. *Cfr*. ARMANDO DIAS RAMOS, O agente encoberto digital… Op. Cit. Pg. 174.

garantias.[309] As provas recolhidas nos canais «abertos», para além de não serem difíceis de recolher e de não exigirem que o agente interaja com os suspeitos, não implicam restrições aos direitos, liberdades e garantias dos indivíduos, uma vez que os conteúdos são colocados pelos próprios sujeitos à disposição de qualquer utilizador que frequente esses espaços cibernéticos comuns. Pense-se, por exemplo, nas informações obtidas através das redes sociais. Embora haja quem questione a validade da prova que tenha sido obtida mediante a aceitação de um "pedido de amizade" pelo suspeito, desconhecendo que o seu utilizador era um agente de investigação, a verdade é que ao aceitar o referido pedido, o suspeito não está sujeito a nenhuma coação, sendo livre de o aceitar ou recusar. Nesse caso o sujeito investigado sabe de antemão que ao aceitar o pedido irá dar acesso a publicações que estão reservadas aos seus "amigos" e dar espaço a qualquer utilizador, inclusivamente a OPC, de obter informações privilegiadas.[310]

Assim como evidencia Lorca Sánchez, embora se pudesse apontar que se o sujeito-alvo tivesse consciência de que aquilo que publicou seria passível de o prejudicar criminalmente, muito provavelmente não teria exposto aquela informação, a verdade é que por muito que as redes sociais contenham informações íntimas, uma vez expostas voluntariamente pelos seus titulares, passam a pertencer à esfera pública, tornando-se acessível a qualquer pessoa.[311]

O mesmo já não acontece com as investigações que decorrem em canais «fechados», em que o agente, grande parte das vezes, para conseguir neles aceder necessita de conquistar a confiança dos potenciais criminosos (regra geral, dos administradores dos grupos), manter uma comunicação estável e prolongada e, até mesmo, praticar atos de caráter supostamente ilícito (como enviar conteúdo ilícito), envolvendo essa operação uma grande dose de engano dos sujeitos investigados.[312] Nestes casos, a autorização judicial e o controlo

---

[309] Neste sentido parece apontar o *Boletín del Ministerio de Justicia de España*, onde se estabelece que as Forças e Corpos de Segurança do Estado espanhol que levem a cabo ações de investigação preventivas na rede pública (isto é, nos canais «abertos» de comunicação) não requerem nenhuma garantia adicional à sua previsão legal, na medida em que se encontram compreendidas dentro das daquelas que são as atribuições próprias desses corpos policiais (previstas nos artigos 282º LECrim e 11.1 LO 2/1986, de 13 de março). *Vide:* Boletín del Ministerio de Justicia – Gobierno español, año LXX. BMJ nº 2186, ISSN: 1989-4767, www.mjusticia.es. *Apud* MARCELO TEMPERINI, MAXIMILIANO MACEDO, Maximiliano, *Nuevas Herramientas… Op. Cit.* Pg. 505.

[310] *Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 173.

[311] MIGUEL ÁNGEL LORCA SÁNCHEZ, *El derecho… Op. Cit.* Pg. 34.

[312] Nas palavras de Pellucci "a infiltração policial em sentido restrito ou próprio é uma técnica especial de investigação sujeita a uma disciplina muito rigorosa, dado o seu caráter potencialmente lesivo de direitos

da operação justificam-se até pelos maiores riscos que existem em a atuação do agente encoberto digital transitar para o domínio da provocação.

Sob outro ponto de vista, poderá ser nos espaços híbridos que se possam levantar as maiores dúvidas. Pensemos, por hipótese, nas situações em que a presença do agente se releve assídua, criando nos utilizadores daqueles espaços reais verdadeiras expetativas jurídicas, bem como nas situações em que o agente comece a desenvolver contactos com os investigados, alcançando as credenciais de acesso a um canal «fechado» de comunicação. Nestes casos é legítimo questionar a partir de que momento a autorização judicial para serem continuadas as investigações cibernéticas se torna imprescindível.

No que a esta questão respeita é consentâneo que a transposição da linha dos canais «abertos» de comunicação, onde atua o agente, para os canais «fechados», lugares privilegiados que requerem uma verdadeira operação de infiltração para neles aceder, pode dar-se de uma hora para a outra. Em face disto, alguns autores, como Frederico Pellucci, entendem que deverão ser considerados "plenamente válidos os contactos prévios anteriores à autorização judicial, aptos a gerar os imprescindíveis vínculos fictícios de camaradagem com os investigados."[313] Ora, entre nós, embora compreendamos que a infiltração policial não possa ser levada a cabo num curto espaço ou através de um único acesso, carecendo efetivamente do estabelecimento de contactos prévios, de modo a gerar a necessária confiança dos investigados e penetrar no espetro criminoso, a verdade é que essa faculdade sem que exista uma prévia autorização judicial habilitante poderá trazer problemas ao nível da validade da prova produzida.

No entanto, reconhecendo que este método oculto de investigação criminal sempre padecerá de dificuldades no que ao plano jurídico-constitucional respeita, optamos por assumir uma posição menos intransigente quanto à validade desses elementos probatórios. Assim, na linha de Frederico Pellucci, consideramos que as informações que, ao vaguear por um canal aberto de comunicação, tenham sido recolhidas pelo agente que, de forma repentina e imprevisível, consegue ter acesso a um canal «fechado» de comunicação, onde eventualmente se estende a prática de um crime cibernético, ainda sem para isso estar munido de uma prévia autorização judicial habilitante, deverão ser alvo de uma ponderação

fundamentais do investigado e de terceiros. De outro lado, essas condições severas não ocorrem quando se trata de operações policiais em canais livres ou abertos". *Cfr*. FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 255

[313] FREDERICO PELLUCCI, *A atuação dos Agentes… Op. Cit.* Pg. 266.

casuística para que possam valer como meio de prova. Atendendo às circunstâncias em que a investigação se desenvolve deverá ser feito um juízo favorável quanto à validade da prova que tenha sido produzida nesses moldes, desde que posteriormente o agente venha a obter a respetiva autorização judicial para atuar naquele campo, como verdadeiro agente encoberto, e se conclua que, de outra forma, a operação estaria condenada ao insucesso. Por outro lado, será ainda importante avaliar o nível de lesão de direitos, liberdades e garantias dos cidadãos investigados: essa lesão deverá ser de tal forma mínima "que quando examinada na balança da ponderação dos valores, nos leva a concluir pela legitimidade da atuação que, posteriormente, veio a ser autorizada como ação infiltrada."[314]

Pense-se, por exemplo, no caso de informações que sejam obtidas através de uma conversação iniciada num *chat «*aberto» e continuada, posteriormente, num canal «fechado» de comunicação, atividade para a qual o agente obteve uma posterior autorização judicial habilitante. Obtida que tenha sido a referida autorização judicial habilitante, do despacho deverão constar alguns pormenores da investigação efetuada, via esclarecedora da validade quer de atos praticados em momento anterior à obtenção da autorização, quer de atos posteriores, tais como: quais os utilizadores dos canais de comunicação cuja investigação é admitida, quais os sistemas informáticos a partir dos quais serão admitidas as atividades investigativas, quais os atos autorizados e não autorizados (para evitar quaisquer tipos de abusos) e ainda quais os *websites*, *chats* ou fóruns (ou outro tipo de canais) autorizados a frequentar, bem como com quem será legítimo interagir e estabelecer contactos mais intensos e duradouros.

6.8. Da imputação de condutas: a possibilidade de desresponsabilização penal do agente encoberto digital pela prática de atos ilícitos

Estando legitimado a atuar de forma mais ativa, munido que esteja de uma autorização judicial habilitante, questiona-se a possibilidade de o agente encoberto digital ser desresponsabilizado por eventuais atos ilícitos que venha a praticar no decurso das suas atividades.

De facto, o art. 6º do RJAE, analogicamente aplicado às atividades do agente encoberto virtual, não esclarece com clareza os limites ao seu *modus operandi*, nada

[314] *Ibidem*. Pg. 268.

prevendo quanto ao que sucederá quando a operação envolva a necessidade da prática de atos cuja ilicitude extravasa os limites da sua desresponsabilização criminal, mas cuja prática se revela a única forma comprovadamente capaz de gerar a confiança dos investigados e, desse modo, penetrar no ambiente criminoso e recolher prova incriminatória.

Como sabemos, o acesso a determinadas plataformas, *websites* ou grupos de c*hat* onde decorrem a prática de crimes está, na maioria das vezes, vedado aos utilizadores comuns. Assim, a admissão nesses grupos, vistos como verdadeiras "ceitas", implica a prestação de uma prova que seja suficientemente credível e capaz de alcançar a confiança dos criminosos, como seja, por exemplo, o envio de ficheiros de conteúdo-ilícito do seu interesse, a troca de informações relevantes (quer informações que contribuem para a prática dos ilícitos, quer informações relativas a uma eventual investigação criminal de que possam desconfiar estarem a ser alvo) ou inclusivamente a prática de qualquer outro ato com relevo jurídico-penal. Neste sentido, Duarte Rodrigues Nunes reconhece ser perfeitamente possível que, no âmbito de uma ação encoberta *online,* o agente tenha, para poder aceder ao cerne criminoso, de partilhar pornografia infantil num *chat* ou fornecer informações sigilosas sobre as investigações em curso, como verdadeiras provas de fidelidade.[315]

Efetivamente, as dificuldades de investigação nas ações encobertas digitais não são equiparáveis às sentidas nas ações encobertas clássicas. Numa ação encoberta tradicional, destinada por exemplo a investigar um potencial crime de tráfico de estupefacientes, o agente poderá facilmente descobrir o local da prática do crime, infiltrar-se no meio criminoso e deter uma perceção visual do espaço que o rodeia, sem que para isso seja necessária a conquista da confiança dos investigados (pense-se nos casos em que o agente possa perseguir os suspeitos e descobrir o local da prática do crime). Dessa forma poderá facilmente confirmar a existência e recolher elementos materiais de prova como documentos, balanças de precisão ou até mesmo o produto estupefaciente.[316] Já quando a investigação decorre em ambiente digital, essa perseguição física não é tecnicamente possível, pelo que o acesso ao *locus delicti* e a identificação do(s) autor(es) do crime só será possível mediante a conquista da confiança dos investigados e, por regra, da prática de atos de natureza também ela ilícita.

Note-se que, como bem evidenciam Stangherlin e Petean, às dificuldades que advêm da identificação da origem da comunicação acrescem, posteriormente, as dificuldades

[315] DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado… Op. Cit.* Pg. 79.
[316] ARMANDO DIAS RAMOS, *A investigação do Cibercrime… Op. Cit.* Pg. 53.

de conexão entre o(s) autor(es) da prática do crime e o proprietário do aparelho eletrónico utilizado. De facto, a ciberinvestigação inicia-se com o rastreamento do IP que permitirá a localização do computador e prossegue com a identificação do seu utilizador (que nem sempre será o seu proprietário), tarefa que, por vezes, se torna algo complexa, na medida em que, na grande maioria das vezes, os crimes são praticados em computadores de uso público (por exemplo, computadores de universidades ou bibliotecas) ou compartilhados por uma família com diversas pessoas.[317]

Assim, em face do exposto, nas palavras de David Silva Ramalho, "a mera identificação dos intervenientes através dos seus *usernames* ou *nicknames*, a partilha de informações confidenciais e anónimas num ambiente onde é patente a falta de confiança entre eles, a acrescer às dificuldades sentidas pelo agente na identificação dos participantes que, no mundo físico, não são percetíveis pela facilidade que tem em fazê-lo pelos seus sentidos (a aparência, a atitude, a voz)" tornam imperativa uma alteração das circunstâncias.[318]

Deste modo, sendo a investigação neste âmbito particularmente difícil, justifica-se que o agente encoberto beneficie, até certa medida, de um regime especial de desresponsabilização criminal por eventuais atos ilícitos praticados, havendo quem lhe aponte uma causa de exclusão da ilicitude, nos termos previstos no art. 6º do RJAE[319]; ou, para casos em que se revele, pela natureza dos atos, impossível a exclusão da ilicitude, a possibilidade de se socorrer de causas de justificação, de exclusão da culpa ou da punibilidade.[320] Porém, a verdade é que, entre nós, não deverá ser admitida uma irresponsabilidade ilimitada.

Não obstante a lei parecer inequívoca quanto à admissibilidade de o agente praticar atos em co-autoria ou como cúmplice, uma tal possibilidade deverá ser aferida à luz do caso concreto: ainda que a lei permita a desresponsabilização penal do agente que pratica atos em autoria material ou em coautoria, se o agente comete um crime por sua livre iniciativa e a sua prática não se revelar necessária em face das circunstâncias objetivamente verificáveis,

[317] MARINA STANGHERLIN, FABIANO AUGUSTO PETEAN, *Agente Infiltrado… Op. Cit*. Pg. 35.
[318] DAVID SILVA RAMALHO, *Métodos ocultos … Op. Cit.* Pg. 295
[319] *Vide*: ponto 4.5. da Parte II.
[320] DUARTE ALBERTO RODRIGUES NUNES, *O problema da admissibilidade …" Op. Cit.* Pg. 893.

a ilicitude não deverá ser naturalmente excluída por via do art. 6.º, n.º 1, da Lei n.º 101/2001.[321]

Por outro lado, deverá ainda ter-se em conta o concreto *modus operandi* do agente. Certas formas de atuação serão menos lesivas do que outras e permitirão alcançar o mesmo efeito útil. Assim, no que esta questão respeita, seguimos de perto o pensamento de F. Bueno de Mata, de acordo com o qual a prática de atos ilícitos com o intuito de conquistar a confiança dos investigados deverá encontrar-se "dentro da margem que a autorização judicial concede e sempre sujeita aos princípios da necessidade e proporcionalidade".[322] Por exemplo, no caso de estarmos perante um eventual crime pedopornográfico, a operação poderá ser levada a cabo mediante o diálogo e a troca de imagens camufladas com atores e atrizes maiores de idade, contratados para o efeito, de modo a não ameaçar, de forma alguma, os direitos das eventuais crianças utilizadas como "isco".[323] De facto, não podemos concordar com situações em que a descoberta da verdade material se sobreponha a bens jurídicos fundamentais como é a proteção da infância.

6.9. As declarações não conscientes: validade da prova produzida em ambiente digital

Esgrimidos os termos em que a ação encoberta digital progride, a questão que agora se impõe relaciona-se com a validade da prova obtida pelo agente encoberto digital. É consabido que a prova alcançada pelo agente encoberto digital é produzida através do emprego de técnicas um tanto desleais, sendo, por regra, o fruto de declarações feitas por quem não estava consciente da identidade do declaratário.

Assim, contra a prova produzida e recolhida nesses moldes vários argumentos se têm apontado: por um lado, que o arguido antes de prestar declarações acerca de factos que lhe estão a ser imputados, deverá ser informado de que goza do direito a não prestar declarações acerca dos mesmos, nos exatos dos arts. 61.º, n.º 1, al. d), 141.º, n.º 4, als. a) e b), 143.º, n.º 2, 144.º, n.º 2, e 343.º, n.º 1*, in fine*, do CPP; por outro lado, aponta-se também que as testemunhas, os assistentes e as partes civis devem ser advertidas da faculdade de não prestarem depoimento, podendo recusar-se a responder a perguntas de que possa resultar a

[321] MANUEL AUGUSTO ALVES MEIREIS, *O Regime das Provas… Op. Cit.* Pg. 164.
[322] FEDERICO BUENO DE MATA, *El agente encubierto en Internet… Op. Cit.* Pg. 306.
[323] *Ibidem.*

sua responsabilidade penal, em conformidade com os arts. 132.º, n.º 2, 134º, 145.º, n.º 3, do CPP, sob pena de as declarações serem insuscetível de ser utilizadas como prova no respetivo processo criminal.

Ora, embora a questão seja complexa, não podemos concordar em pleno com os argumentos anteriores, quando pensados à luz das concretas ações encobertas digitais. À semelhança do defendido por Duarte Rodrigues Nunes, entendemos que estas normas estão pensadas para proteger a posição processual dos sujeitos no âmbito de um interrogatório formal, não sendo, portanto, diretamente aplicáveis às declarações prestadas no âmbito de uma ação encoberta.[324]

De facto, um juízo desfavorável relativamente à prova obtida nesse contexto seria negar utilidade prática às ações encobertas, nem sequer fazendo sentido, nesse caso, a sua previsão e regulamentação enquanto verdadeiro método de obtenção de prova. Note-se que, como bem evidencia o autor *supra* referido, as atividades do agente encoberto consistem em precisamente, ocultando a sua verdadeira identidade, "ver e ouvir o que acontece à sua volta", o que incluirá naturalmente também os depoimentos daqueles que investiga.[325]

Deste modo, quando o investigado confessa ao agente encoberto determinados factos que poderão constituir motivo da sua responsabilização criminal, não estando consciente de que está efetivamente perante uma autoridade, fá-lo de forma livre, sem estar sujeito a qualquer tipo de coação ou pressão psicológica, como se de uma confissão a qualquer outra pessoa se tratasse (ou seja, tudo decorre como em qualquer conversa normal entre dois sujeitos).[326] Do que resulta que, nas palavras de Armando Dias Ramos, à semelhança do que sucede na interceção de escutas telefónicas, em que o suspeito fala abertamente, nas ações encobertas opera a mesma liberdade, sendo as provas recolhidas o fruto de uma prática que o agente levaria a cabo de qualquer forma (independentemente de qualquer atividade do agente), não podendo o *nemo tenure* ter uma natureza absoluta.[327]

Ademais, idêntico juízo deverá também ser feito relativamente à prova que seja produzida e recolhida através da chamada técnica da «*engenharia social»,* isto é, práticas que podem ser utilizadas para o acesso a informações/dados pessoais de pessoas singulares ou coletivas, mediante o cruzamento de informações entre diversas páginas, onde se obtém

[324] DUARTE ALBERTO RODRIGUES NUNES, *O agente infiltrado … Op. Cit.* Pg. 59.
[325] *Ibidem.*
[326] *Ibidem.*
[327] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 100.

informação acerca da pessoa e dos seus gostos e por tentativa/erro se consegue aceder ao seu correio eletrónico ou a outras informações relevantes. Tratam-se, portanto, de práticas que permitem a recolha de prova que é cedida pelos próprios suspeitos investigados, de forma não intencional, sem que disso se apercebam. Em ambiente informático-digital, a engenharia social tem-se revelado determinante para*, v.g*, proceder à identificação do IP que determinado suspeito utiliza ou outro tipo de informação relacionada com a prática do crime (que sistema operativo tem instalado, que *browser* e versão utiliza no seu equipamento, entre outras).[328]

Feitas estas considerações, cumpre relevar, em jeito conclusivo, que, na verdade, as próprias regras do interrogatório formal e do princípio *nemo tenetur se ipsum accusare,* amplamente defendidas por Costa Andrade[329], nunca chegariam a ser feridas neste âmbito, na exata medida em que as atividades do agente encoberto se localizam temporalmente numa fase processual anterior, isto é, numa fase em que nem se coloca a questão de os sujeitos investigados poderem recusar-se a prestar declarações. Note-se que, inclusivamente, estando em causa uma ação encoberta desencadeada para a prossecução de fins preventivos, as pessoas investigadas ainda nem sequer figuram como verdadeiros sujeitos processuais, não ocupando, portanto, a posição de arguido, testemunha ou assistente, que lhes atribua a faculdade de exercer certos direitos processuais, como seja a recusa de depoimento. De maneira que, como evidencia Armando Dias Ramos, a materialização formal da constituição de arguido se revela fulcral, pois só nesse momento o suspeito adquire consciência de que está a ser efetivamente investigado. No entendimento do autor, antes da constituição de arguido o suspeito não detém o estatuto de sujeito processual, não se podendo defender.[330]

Pelo exposto, saem, assim, frustrados aqueles argumentos. Não vemos, pois, razões para invalidar uma prova que é obtida através de um método de investigação criminal que está legalmente previsto e que decorre nos moldes legalmente previstos. Ressalvamos apenas, obviamente, que juízo diferente deverá ser feito quando o suspeito, no decurso da ação encoberta, seja incitado ou induzido à prática do crime, em violação do primado do art. 32º/8 da CRP[331].

---

[328] *Ibidem.* Pg. 169 e 170.
[329] MANUEL DA COSTA ANDRADE, *Bruscamente no verão passado… Op. Cit.* Pg. 544 a 554.
[330] *Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 100.
[331] *Ibidem.*

6.10. Problemas (in)ultrapassáveis: os concretos direitos fundamentais restringidos e os limites à descoberta da verdade material na realidade digital

Não obstante as ações encobertas se reputarem como um método de investigação criminal essencial para fazer prova de determinados factos ilícitos, não podemos deixar de considerar estar em causa uma "técnica de investigação de moral duvidosa"[332], atendendo ao facto de ser o próprio suspeito que, atuando em erro sobre a qualidade do agente, produz involuntariamente, a prova da sua própria condenação[333]. É incontestável que este modo de investigação acarreta a possibilidade de serem feridos importantes princípios processuais, como o da lealdade inerente ao processo penal e o do processo justo e equitativo, sobretudo, quando estamos nos limites transfronteiriços entre a infiltração e a provocação.

De facto, embora não seja admitida entre nós a figura do agente provocador, o papel assumido pelo agente encoberto no nosso ordenamento não está bem definido: constatamos a possibilidade de este poder praticar atos que possam levar o investigado – de uma forma ou de outra - a revelar-se quanto a crimes que já tenha praticado ou venha a praticar. Por outro lado, o próprio regime jurídico vigente abre espaço à prática de atos pelo agente que possam induzir o investigado em erro relativamente à sua identidade e possam promover relações próximas com o criminoso, com o objetivo final de conquistar a sua confiança e, por essa via, ter acesso a informações e outras confidências.

Ora, presidindo ao nosso processo penal um princípio da não autoincriminação, de acordo o qual "o acusado não está obrigado a contribuir para a sua própria incriminação, não recaindo sobre ele o dever de colaborar na descoberta da verdade material"[334], muito se tem questionado sobre a legitimidade destas operações.

Deste modo, no âmago da questão está efetivamente saber se e quando estamos perante um método proibido de obtenção de prova, enquadrável no artigo 126º do CPP,

---

[332] MANUEL MONTEIRO GUEDES VALENTE, *Teoria Geral… Op. Cit.* Pg. 406.
[333] FERNANDO GONÇALVES, JOÃO MANUEL ALVES, *Crime. Medidas de Coação e Prova… Op. Cit*. Pg. 300.
[334] MARIA JOÃO ANTUNES, *Direito ao silêncio e leitura em audiência de declarações do arguido*, in SubJudice, Justiça e Sociedade, n. º4, setembro/dezembro 1992. Pg 26. Também neste sentido: PAULO PINTO DE ALBURQUERQUE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* 2ª Ed., Universidade Católica Editora, Lisboa, 2008. Pg. 48 e 183;

preceito que ao estipular expressamente que "são nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas", se assume como a "*norma processual fundamental* de garantia dos direitos fundamentais das pessoas que se vêem implicadas em investigações criminais"[335]. No entanto, importa, *ex ante,* para a compreensão do preceito, o apuramento do seu ânimo jurídico.

De acordo com a corrente maioritária, onde se insere Susana Aires de Sousa, a norma tem como fundamento a necessidade de dar proteção às garantias processuais do arguido, nomeadamente da dignidade humana e da liberdade de participação e contributo em matéria probatória.[336] No fundo, estabelece a autora que a referência do legislador à proibição do uso de meios enganosos tem como principal objetivo o repúdio de métodos de investigação que coloquem em causa a liberdade de decisão do investigado mediante um engano eficaz que o transforma "num meio de prova contra si próprio".[337] Do que resulta que, nas palavras de Figueiredo Dias, "só no exercício de uma plena liberdade de vontade pode o arguido decidir se e como deseja tomar posição perante a matéria que constitui objeto do processo"[338].

Sucede que, se é verdade que a norma se mostra explícita quanto aos seus objetivos e fundamentos, ela não fornece, contudo, critérios suficientemente claros que nos permitam indagar quando estará em causa um verdadeiro caso de engano, na medida em que, pela

---

[335] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos… Op. Cit.* Pg. 585. (o itálico não é nosso)

[336] *Cfr.* SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit.* Pg. 1215.

[337] *Ibidem.* Pg. 1216; Também neste sentido: FERNANDO GONÇALVES, MANUEL JOÃO ALVES, MANUEL MONTEIRO GUEDES VALENTE, *Lei e Crime: O agente infiltrado versus o agente provocador… Op. Cit.* Pg. 126: "Num processo caracterizado com a máxima acusatoriedade, o arguido não pode ser concebido como um objecto do processo, não sendo alguma vez meio formal de prova, mas deve ser encarado como um sujeito processual que possa livremente contradizer a acusação, recorrendo a armas iguais às de acusador. Do exposto decorre que o arguido não pode ser obrigado a prestar qualquer colaboração com o tribunal, devendo a sua participação no processo ser livre, respeitando-se a sua integral vontade de forma que não surja uma verdade deturpada por força de qualquer pressão". Com semelhante entendimento se manifesta Benjamim Silva Rodrigues, ao considerar que "o processo penal não parte do pressuposto de que o arguido seja considerado (,mais,) um «*objeto do processo»,* já que *(se)* lhe reconhece o estatuto de *sujeito processual* guindado com um leque de direitos e garantias (processuais e) fundamentais impostergáveis, de tal modo que a prova obtida contra tais garantias processuais "inquina", geralmente, tal acervo probatório e a leva ao altar da "*prova proibida"* e insuscetível de qualquer aproveitamento ou *valoração." Cfr.* BENJAMIM SILVA RODRIGUES*, Da Prova Penal: Novos Métodos "Científicos"… Op. Cit.* Pg. 49 (os itálicos não são nossos).

[338] FJORGE DE FIGUEIREDO DIAS, *Sobre os Sujeitos Processuais no Novo Código de Processo Penal, in* Jornadas de Direito Processual Penal, O Novo Código de Processo Penal, Centro de Estudos Judiciários, Coimbra: Almedina, 1991. Pg. 27 e 28.

forma como está redigida, podem nela caber inúmeras situações, "desde a simples astúcia até às formas de engano mais próximas da coação".[339] E é em face disso que Sandra Oliveira e Silva, procurando decompor o conceito de «engano proibido», estabelece que estaremos na presença de um meio enganoso sempre que o investigador: "(1) de forma deliberada e intencional, (2) crie ou aprofunde uma falsa representação da realidade ou imita um dever de informação legalmente imposto, (3) perturbando de forma grave a liberdade de vontade do arguido e determinando-o à prestação de informações probatórias".[340] Susana Aires de Sousa acrescenta que só estaremos perante um meio enganoso se se produzir um nexo de causalidade entre o engano derivado da ocultação da identidade do agente e os meios de prova obtidos, "não basta[ndo], sem mais, a existência de erro criado pelo agente policial"[341].

Nesta ordem de ideias, cumpre evidenciar que esta questão se revela particularmente expressiva no âmbito das ações encobertas que se desenrolam em ambiente digital. De facto, neste concreto contexto, somos levados a questionar: deverá o engano derivado da ocultação da identidade do agente (que, como vimos, é inerente à própria natureza) ser suficiente para se concluir pela presença de meio enganoso de obtenção de prova? Entendemos que não.

Assim, entre nós, acompanhando o entendimento das autoras *supra* citadas, um método enganoso de obtenção de prova existirá sempre - e só - nos casos em que, por força do engano, se tenha conseguido produzir prova incriminatória. Por outro lado, sempre que *in casu* se verifique a presença de factos anteriores à ação encoberta indiciadores de que o crime sempre viria a ser cometido, não podemos enveredar pela nulidade da prova obtida por um suposto agente reputado de provocador. Isto porque, tal como denota Susana Aires de Sousa, estaremos perante "casos em que sem a atuação enganosa do agente policial, o suspeito sempre teria possivelmente ou provavelmente praticado o crime, não se podendo imputar ao engano sobre a pessoa do provocador, a atuação do provocado"[342]. Referimo-nos, resumidamente, a situações em que a liberdade de vontade ou de decisão do investigado em praticar o crime não é afetada de forma alguma pela ação do agente encoberto (na medida

[339] *Ibidem.* Pg. 1218.
[340] SANDRA OLIVEIRA E SILVA, *O Arguido como Meio de Prova contra si mesmo: Considerações em torno do princípio nemo tenetur se ipsum accusare*. Coimbra: Editora Almedina, 2019 (Reimpressão). Pg. 518.
[341] SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit.* Pg. 1233.
[342] *Ibidem*. Pg. 1234.

em que a ação já havia sido previamente pensada e planeada pelo primeiro), limitando-se o agente a promover a descoberta de uma verdade inevitável.

Sobre esta questão e no sentido que aqui propugnamos, também se pronunciou o Tribunal Constitucional no Acórdão nº 578/98 de 14 de outubro, onde estabeleceu que "o que verdadeiramente importa (…) é que o funcionário de investigação criminal não induza ou instigue o suspeito à prática de um crime que de outro modo não praticaria ou que não estivesse já disposto a praticar" [343].

Apontamos ainda o facto de não fazermos uma interpretação literal do artigo 126º do CPP que repudia todo e qualquer meio de prova que tenha sido obtido com recurso ao engano - seja ele quanto à ação ou à pessoa do agente -, uma vez que isso levar-nos-ia a pugnar pela inadmissibilidade de tais provas em termos absolutos. Assim, entre nós, o que determinará a nulidade da prova será o facto de ter sido conseguida através de um engano, não o facto de o agente a ter alcançado mediante a ocultação da sua identidade - o que, aliás, já vimos ser legalmente admissível, ao abrigo do art. 4º do RJAE. Também nesta mesma linha de pensamento se posiciona o TC no Acórdão anteriormente mencionado, onde estipula expressamente que "a nulidade das provas [se] afere quanto ao modo objetivo da sua obtenção, não respeita[ndo] à qualidade do agente que as produz ou recolhe."[344] Do que resulta, assim, que qualquer prova que seja obtida pelo agente, ainda que com recurso a uma identidade fictícia, sem que entre no campo da provocação, seja admissível. No mesmo sentido nos parece também ter avançado Susana Aires de Sousa quando refere que "não releva o engano sobre a qualidade do agente investigador, por impossibilidade de afirmar o nexo de causalidade entre a aparência criada e a prática do facto com ressonância criminal, nas situações em que o agente se limita a estar presente sem influir na intenção criminal do suspeito."[345]

Feitas estas considerações, podemos ainda inferir que ainda que admissíveis, nos termos anteriormente expostos, as ações encobertas pressupõem sempre, inevitavelmente, a colisão entre dois interesses antagónicos: por um lado, a descoberta da verdade material e realização da justiça; por outro, a defesa de direitos fundamentais dos cidadãos, sendo a

---

[343] Acórdão do TC nº578/98 de 14 de outubro. Disponível em http://www.pgdlisboa.pt/jurel/cst_main.php?ficha=9321&pagina=310&nid=3845 [Acesso em: 4 jan. 2022].
[344] ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 137
[345] SUSANA AIRES DE SOUSA, *Agent Provocateur… Op. Cit.* Pg. 1234.

restrição dos direitos, liberdades e garantias em "ambiente digital ou eletrónico" de "especial intensidade", dada a quantidade de informações a que os sistemas informáticos possibilitam ter acesso.[346]

De facto, os atuais moldes da criminalidade determinam a impossibilidade de um processo probatório sem qualquer tipo de ingerência naquilo que será o núcleo dos direitos, liberdades e garantias dos sujeitos investigados. Significa isto que o desencadeamento de qualquer ação encoberta exige a ponderação dos interesses envolvidos e a verificação*, in casu*, de qual o interesse prevalecente – se a realização da justiça, com a inerente restrição de direitos fundamentais, ou se o respeito por direitos constitucionalmente reconhecidos aos cidadãos investigados, com prejuízo para a descoberta da verdade material.[347]

Note-se que a própria CRP acaba por confirmar o entendimento anterior ao prever a admissibilidade deste método de investigação mesmo quando ele implique a restrição de determinados direitos fundamentais. Veja-se o seu art. 18º nº 2 que ressalva apenas o facto de "as restrições [deverem] limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos." De relevar que a restrição que aqui pugnamos não se estende, naturalmente, a determinados bens jurídicos como a vida e integridade física, tendo em conta que esses constituem bens jurídicos primários que nunca deverão poder ser colocados em causa em prol de uma suposta descoberta da verdade.[348] Assim, na linha de Alves Meireis, consideramos que as atividades do agente encoberto serão admissíveis desde que pautadas pelos limites do consentido pela ideia de Estado de Direito Democrático, isto é, desde que respeitem os princípios da legalidade, da necessidade, da proporcionalidade,

---

[346] MANUEL MARCHENA GOMÉZ, NICOLÁS GONZÁLEZ-CUÉLLAR SERRANO, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid: Ediciones Jurídicas Castillo de Luna, 2015. Pg. 386 *Apud* JULIANA FILIPA SOUSA CAMPOS, O *Malware … Op. Cit.* Pg. 55.

[347] No mesmo sentido, David Silva Ramalho, constatando a impossibilidade de se conceber um sistema processual penal eficaz sem qualquer ingerência nos direitos fundamentais dos cidadãos, entende que haverá que se procurar um equilíbrio entre o interesse do Estado na prossecução penal dos culpados e a tutela adequada dos direitos, liberdades e garantias dos cidadãos. Acrescenta ainda que "o equilíbrio não deve, porém, ser confundido com a igualdade dos pesos em ambos os pratos de uma balança, mas antes como justa ponderação do sacrífico parcial indispensável e constitucionalmente aceitável de um polo em função do outro" (*Cfr.* DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 183).

[348] De acordo com Isabel Oneto, "a opção axiológico-constitucional de prevalência da dignidade humana se impôs como referência obrigatória para o legislador". Para além dos bens jurídico-penais vida e integridade física referidos por nós, a Autora acrescenta ainda a intimidade da vida privada e a honra como bens jurídicos que também não podem sofrer lesões na sua esfera em função de uma suposta eficácia da investigação criminal. Já como bens jurídicos sujeitos a menor intensidade de proteção penal a Autora aponta os relacionados com a esfera patrimonial. (*Cfr*. ISABEL ONETO, *O Agente Infiltrado… Op. Cit*. Pg. 183).

não violem o núcleo essencial dos direitos afetados e não sejam reconduzíveis ao domínio da provocação.[349]

Não negamos, porém, que as ações encobertas digitais produzem incontornáveis bloqueios à proteção completa dos direitos dos visados, tanto no plano processual, como ao nível dos próprios direitos fundamentais. A ingerência nos direitos fundamentais dos investigados nas ações encobertas digitais é tal de forma complexa que David Silva Ramalho equaciona se deverá existir uma tutela distinta para cada sistema informático consoante "o mesmo se encontre fisicamente no domicílio do visado ou noutro local, contenha dados pessoais ou mesmo íntimos, os dados se encontrem armazenados no sistema ou simplesmente sejam apreensíveis através dele ou caso contenha correspondência digital"[350]. Assim, o facto de as atividades do agente abrangerem formas de atuação distintas, com diferentes repercussões no âmago dos direitos fundamentais dos sujeitos investigados, poderia motivar diferentes especificações legais.

Chegados a esta conclusão, cumpre-nos analisar em que termos a ação encoberta digital poderá colidir com os direitos fundamentais dos cidadãos investigados e se a referência, por analogia, à restrição de certos – e concretos – direitos fundamentais mantém a sua lógica quando em causa está uma atividade investigativa em ambiente digital. De facto, como nota Benjamim Silva Rodrigues, os novos métodos de investigação (em que se inserem naturalmente as ações encobertas digitais) proporcionados pelo progresso científico fizeram com que, por um lado, os velhos direitos fundamentais se "modernizassem" e, por outro, surgissem novos direitos fundamentais ou novas dimensões (até aqui desconhecidas) dos velhos direitos fundamentais.[351]

Sendo a prova obtida através da invasão dos sistemas informáticos dos sujeitos investigados, questiona-se como pode ser gerida a expetativa de inviolabilidade dos respetivos sistemas, dos dados automaticamente gerados pelos sistemas, dos ficheiros armazenados ou dos dados guardados na nuvem. Efetivamente, se a validade da prova alcançada pelo agente encoberto físico já era alvo de controvérsia, pelo facto de contender diretamente com os direitos, liberdades e garantias dos cidadãos investigados, essa questão

[349] MANUEL AUGUSTO ALVES MEIREIS, *Homens de confiança* in II Congresso de Processo Penal, Lisboa: Almedina, 2006. Pg. 97.
[350] DAVID SILVA RAMALHO, *Métodos ocultos … Op. Cit.* Pg. 242.
[351] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos… Op. Cit.* Pg. 71 e 72.

levanta-se com ainda maior afinco no âmbito das ações encobertas digitais, onde ganham expressão novos direitos fundamentais.

Neste sentido, David Silva Ramalho alude a um novíssimo direito especialmente afetado no âmbito das ações encobertas digitais: o direito à integridade e à confidencialidade dos sistemas informático-digitais.[352] De acordo com o autor, este direito visa, por um lado, "garantir que os dados gerados (propositadamente pelo utilizador ou automaticamente pelo sistema), tratados e armazenados pelos sistemas informáticos permaneçam confidenciais, e, por outro, que a integridade do sistema não seja comprometida através de acessos não autorizados por parte de terceiros"[353]. É, portanto, um direito fundamental cujo núcleo de proteção incide, essencialmente, sobre sistemas informáticos que possam conter dados pessoais do visado, capazes de permitir o conhecimento significativo da sua vida pessoal ou informações detalhadas da sua personalidade (*v.g.* computadores portáteis, telemóveis, *webmails* ou outros serviços de computação em nuvem acessíveis a partir do sistema inicial). Nas palavras de Juliana Campos, este direito corresponde, resumidamente, a uma importante garantia de proteção dos indivíduos contra o acesso oculto através de todo e qualquer sistema de tecnologia de informação.[354]

A par do direito à integridade e à confidencialidade dos sistemas informático-digitais, fala-se ainda neste âmbito de um outro: o direito à autodeterminação informacional (art. 26º, nº1 e art. 35º da CRP). De facto, embora a ação encoberta digital possa abranger informações/ dados pessoais que o próprio sujeito investigado tenha colocado, livremente, ao dispor do conhecimento público (e, por consequência, das autoridades policiais), entende-se que, por vezes, esse direito à autodeterminação informacional acaba por ser restringido porquanto o seu titular perde o controlo de quando e que em extensão as referidas

---

[352] Para a emergência deste novo direito fundamental, verdadeiramente capaz de tutelar a vida privada dos cidadãos investigados contra acessos do Estado nos sistemas informáticos, alertou o Tribunal Constitucional alemão, em 27 de fevereiro de 2008 (*Vide*: BverfG, 1 BvR 370, 595/07, disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html [Acesso em: 16 de maio de 2022],)

[353] DAVID SILVA RAMALHO, *Métodos ocultos … Op. Cit.* Pg. 247

[354] De acordo com a Autora este direito apenas é violado se houver a expetativa de que o visado utiliza aquele concreto sistema informático. No seu entender, atendendo a redação da CRP, poderá ter-se essa garantia como uma extensão do direito ao desenvolvimento da personalidade, na sua dimensão de liberdade; do direito à autodeterminação informacional, contra a revelação dos dados pessoais sem que para isso o utilizador tenha dado o seu livre e esclarecido consentimento e do direito à reserva da intimidade da vida privada e familiar, na medida em que há possibilidade de acesso a informações que se integrem nesse âmbito. *Cfr.* JULIANA FILIPA SOUSA CAMPOS, O *Malware… Op. Cit.* Pg. 57 a 60.

informações pessoais são reveladas, recolhidas e utilizadas para outros fins, em prejuízo próprio (*v.g.* de investigação criminal). Em suma, está, assim, em causa, a possibilidade de as ações encobertas digitais limitarem o direito de cada cidadão a *"ser ele próprio a decidir quando e dentro de que limites os seus dados pessoais podem ser revelados"*.[355]

Note-se, porém, que não apenas de "novos" direitos como os anteriormente enunciados são passíveis de ser restringidos pelas operações do agente encoberto digital. À semelhança do que sucede nas ações encobertas tradicionais, a efetivação e sucesso das ações encobertas digitais implicam igualmente limitações a importantes direitos fundamentais tradicionais, já francamente mais conhecidos, em concreto: o direito à proteção da vida privada e da família (art. 26º CRP); direito à inviolabilidade do domicílio e da correspondência (art. 34º da CRP); e, em geral, o direito ao livre desenvolvimento da personalidade.[356] Não obstante, importa perceber em que dimensão e com que extensão, sobretudo quando em causa está o direito à inviolabilidade do domicílio e da correspondência.

No que respeita concretamente ao direito à inviolabilidade do domicílio, é natural que, nas ações encobertas clássicas, o agente encoberto necessite de proceder a atos de transposição das barreiras físicas da propriedade privada de um suspeito para ver, ouvir, ou simplesmente obter alguma informação essencial à investigação que nela se encontre. Trata-se, pois, de um direito que pretende efetivar a proteção do próprio espaço físico da privacidade (no seu sentido literal).

Ora, embora, à primeira vista, pudéssemos ser levados a pensar que, pela natureza e circunstâncias em que a ação encoberta digital decorre, a atuação do agente não fosse capaz de lesar o direito à inviolabilidade do domicílio, a questão não pode ser tomada de forma tão

---

[355] *Cfr.* GOSSEL KARL-HEINZ, *As proibições de prova no direito processual penal in* Revista Portuguesa de Ciência Criminal, julho-setembro de 1992. Pg. 432. Sobre esta questão, também se debruçam: HELENA MONIZ, *Notas sobre a protecção de dados pessoais perante a informática in* Revista Portuguesa de Ciência Criminal, abril-junho de 1997. Pg. 245 a 261; *Idem*, *Os problemas jurídico-penais da criação de uma base de dados genéticos para fins criminais in* Revista Portuguesa de Ciência Criminal, abril-junho de 2002. Pg. 246 e 247; SÓNIA FIGALDO, *Determinação do perfil genético como meio de prova em processo penal*, in Revista Portuguesa de Ciência Criminal, janeiro-março de 2006. Pg. 127; SÓNIA FIGALDO, *A utilização de inteligência artificial… Op. Cit.* Pg. 138; RITA CASTANHEIRA NEVES, *As ingerências nas Comunicações Electrónicas… Op. Cit.* Pg. 58 e ss.; Ac. do TC nº 155/2007.

[356] *Cfr*. J.J. CANOTILHO, VITAL MOREIRA, *Anotação ao art. 26º in* Constituição da República Portuguesa Anotada, vol. I, 4ª Ed. Revista, Coimbra: Coimbra Editora, 2007. Pg. 463 e ss.

linear.[357] De facto, a violação do domicílio, "enquanto espaço de afirmação da privacidade espacial íntima"[358], é hoje possível sem que haja uma invasão propriamente física e corpórea das fronteiras erguidas pelas paredes e pelo telhado, através de uma penetração "eletrónica-digital" verdadeiramente capaz de captar a "alma digital" do visado.[359] Nesse sentido, Benjamim Silva Rodrigues aponta que "terão, agora, aptidão agressiva de tal direito fundamental, toda a forma de devassa que seja levada a cabo mediante a introdução e presença, no domicílio, de meios técnicos de escuta, de transmissão de imagens ou de sons por intermédio de sofisticados meios de captação acústica e visual à distância"[360], restando apenas compreender de que forma e com que alcance.

Ora, como explica Juliana Campos, o apuramento da violação do direito à inviolabilidade do domicílio através do uso de *malware,* uma possível forma de atuação do agente encoberto digital, dependerá da funcionalidade concretamente utilizada e da forma de instalação: se o programa tiver sido instalado remotamente e for utilizado com o fito de recolher prova interna constante do sistema informático, não há suscetibilidade de aquele direito ser comprimido, na medida em que, não obstante o referido sistema informático estar localizado no interior da residência do visado, o «espaço físico da esfera privada», a que

[357] Desde logo, dúvidas se colocam quanto à amplitude do objeto da garantia constitucional da inviolabilidade do domicílio. Autores há que adotam uma conceção de domicílio mais ampla: Gomes Canotilho e Vital Moreira, encontrando dificuldades na sua definição, entendem que o conceito deverá abranger não só o local onde se habita de forma habitual e/ou principal (isto é, a residência habitual em sentido civilístico, que não deverá excluir a residência precária como as tendas e as *roulotes*), mas também temporária e/ou secundária (como, por exemplo, os quartos de hotel), bem como os locais de trabalho (como os escritórios). No seu entendimento, dada a sua função constitucional, esta garantia deverá estender-se quer ao domicílio voluntário geral quer ao domicílio profissional (nos termos dos arts. 82º e 83º do CC), assim como deverá se estender à sede das pessoas coletivas. *Cf.* J.J. CANOTILHO, VITAL MOREIRA, *Anotação ao art. 34º in* Constituição da República Portuguesa Anotada, vol. I, 4ª Ed. Revista, Coimbra: Coimbra Editora, 2007. Pg. 540 e 541). Também neste sentido: MANUEL MONTEIRO GUEDES VALENTE, *Processo Penal, Tomo I*, 2010. Pg. 401; Já outros Autores, enveredando num sentido mais restritivo do conceito, entendem que o direito à inviolabilidade do domicílio não pode estender-se a lugares não habitacionais ou à sede de pessoas coletivas. J. Martins da Fonseca considera que a noção constitucional de domicílio deverá apenas abarcar a «casa ou parte de uma casa que um indivíduo ocupa, de facto, num dado momento, para aí viver só ou com os membros da sua família» (*vide:* J. MARTINS FONSECA, *O Conceito de Domicílio, face ao Art. 34º da Constituição da República, in* Revista do Ministério Público, nº 45, ano 12º, 1991. Pgs. 45 e segs.); Na mesma linha de pensamento, veja-se ainda: JOÃO CONDE CORREIA, *Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art.º 32.º, n.º 8, 2ª parte, da C.R.P.)?, in* Revista do Ministério Público, ano 20.º, n.º 79, 1999. Pg. 51; Acórdão do TC nº 364/2006.

[358] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos… Op. Cit.* Pg. 329.

[359] *Ibidem.*

[360] *Ibidem.* Pg. 479 e 480.

alude Costa Andrade, se mantém intocável[361]; já se, diferentemente, houver uma ultrapassagem propriamente dita dos limites físicos da propriedade do visado, aquele direito será inelutavelmente restringido. Nota ainda a autora que, de igual modo, a violação da garantia ocorrerá sempre que houver lugar à ativação de funcionalidades que possibilitam a recolha de prova externa, como é exemplo a ativação de um microfone ou uma câmara do investigado, dado que, ainda que efetuada à distância, permite a devassa da esfera privada.[362]

Assim, à semelhança do que sucede com o uso de *malware,* não obstante a ação encoberta digital ser beneficiada pela ausência de fronteiras físicas, não deixa, por essa razão, de revelar-se apta a colidir com aquele direito. Efetivamente, de acordo com alguma doutrina, a invasão do domicílio, para além de poder operar-se por via da ultrapassagem física, acústica ou ótica, poderá também efetivar-se através de novos meios técnicos, sem que a entrada na esfera privada implique uma presença propriamente física do agente.[363]

Neste sentido avança também Armando Dias Ramos ao refletir sobre, por exemplo, o uso de *drones*, pelo agente encoberto, na investigação criminal. Admitindo que o uso do *drone*, em substituição à presença física do agente, no desempenho de determinadas tarefas possa ser mais profícuo e levantar menos suspeitas, o autor questiona em que situações tal não se deverá considerar *contra legem.* De acordo com o autor, se o uso do *drone* for feito com o objetivo de apenas proceder ao reconhecimento do local, de maneira a conseguir alcançar-se uma perspetiva diferente de uma zona, que posteriormente possa ser alvo de uma busca ou localização de um suspeito, nada haverá a opor; mas se, ao invés, o aparelho for utilizado, através das janelas da residência onde se encontra o investigado, com a intenção de captar imagens ou sons ou para disseminar *benware*[364] (mediante a ligação a redes *wifi* ou o *sniffer* de pacotes de dados, isto é, a interceção e posterior reorganização dos pacotes de dados, tornando a informação legível), e, dessa forma, conseguir penetrar nos sistemas informáticos do visado e obter prova incriminatória, tal já não deverá ser admissível.[365]

---

[361] MANUEL DA COSTA ANDRADE, *Comentário ao art. 190º in* Comentário Conimbricense do Código Penal: Parte Especial (dir. Jorge Figueiredo Dias), Tomo I, 2ª Ed., Coimbra: Coimbra Editora, 2012. Pg. 1018 e ss;

[362] JULIANA FILIPA SOUSA CAMPOS, *O Malware … Op. Cit.* Pg. 61 e 62.

[363] *Ibidem.*

[364] Expressão utilizada pelo Autor para fazer referência à designação, mais comumente conhecida, de "*malware*".

[365] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 222 e 223.

De relevar ainda que, Juliana Campos, na esteira de Costa de Andrade, entende que a violação do direito à inviolabilidade do domicílio não implica necessariamente a violação do direito à privacidade/intimidade, pois este último tomado em sentido material, apenas se poderá considerar violado se algo de "privado" for observado ou descoberto, "actualiza[ndo]-se e exprim[indo]-se muito para além das quatro paredes".[366]

Feitas estas considerações, cumpre agora analisar a aptidão das ações encobertas digitais na violação do direito à inviolabilidade da correspondência. Como bem elucida Costa Andrade, a correspondência segue, na sua generalidade, fechada, isto é, pressupõe um procedimento que estabelece um obstáculo físico à tomada de conhecimento e que só é ultrapassável à custa de uma atividade física[367], como a rutura material do envelope de uma carta. Ora, estando, assim, também uma tal garantia embutida numa referência a um certo espaço físico da esfera privada, questiona-se se fará sentido considerar-se um ato de violação da correspondência o acesso a *e-mails* ou mensagens trocadas em fóruns de discussão ou c*hats* privados, no âmbito de uma ação encoberta digital.

Note-se que a questão se reveste de sentido, uma vez que, nas palavras de David Silva Ramalho, embora seja possível a extensão da tutela jus-fundamental a cada um dos bens jurídicos subjacentes às atividades do agente encoberto digital, nuns casos de modo mais forçado do que noutros, à luz dos direitos, liberdades e garantias já existentes, "esta tutela fragmentária assenta numa tentativa de encaixe, por vezes frágil, de novas realidades em conceitos para os quais não foram concebidos."[368] Ora, é em face desta "tentativa de encaixe frágil" e desajustada que Armando Dias Ramos pugna pela alteração do art. 17º da LC, referente à apreensão de correio eletrónico e registos de comunicações de natureza semelhante, constatando que um *e-mail* não pode ser equiparado à correspondência tradicional, porquanto gravitam em realidades distintas.[369]

---

[366] JULIANA FILIPA CAMPOS SOUSA, *O Malware… Op. Cit.* Pg. 62; MANUEL DA COSTA ANDRADE, *Anotação ao Acórdão nº 364/2006, de 8 de junho (Domicílio, Intimidade e Constituição),* RLJ, ano 138º, nº 3953, novembro/dezembro de 2008. Pg. 109.

[367] MANUEL DA COSTA ANDRADE, *Anotação ao artigo 194º do CP – Violação de correspondência ou de telecomunicações, in* Comentário Conimbricense do Código Penal, Tomo I, 2ª Edição, 2012. Pg. 1092.

[368] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 242.

[369] ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 267; Também no sentido da impossibilidade de equiparação do correio eletrónico à correspondência tradicional quer do ponto de vista operacional, quer técnico, veja-se ainda: DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Cit*. Pg. 140 a 145; Note-se que esta alteração já esteve "em cima da mesa" em 2021, tendo alcançado a aprovação da AR pelo Decreto nº 167/XIV mas sido vetada pelo PR, em sede de fiscalização preventiva da constitucionalidade pelo TC. Na prática, esta alteração legislativa permitiria ao Ministério

Assim, por tudo quanto atrás ficou dito, é forçoso concluir que os locais e os contextos tradicionais da proteção da vida privada, como o domicílio (físico) e a correspondência (corpórea), já não correspondem à essência da privacidade individual que hoje se estende a planos não palpáveis, sendo notória a atual desadequação das normas que regulam a possibilidade de intromissão na privacidade com finalidades de investigação criminal informático-digital.[370]

7. Que futuro para as ações encobertas digitais? Considerações finais.

Reconhecidas, por um lado, as dificuldades convocadas pelas ações encobertas digitais, enquanto método oculto de investigação criminal, ao nível da ingerência dos direitos, liberdades e garantias dos cidadãos investigados e, por outro, a forma como determinados conceitos como o de «privacidade», «domicílio» e de «espaço» se encontram desfasados daquilo que será a realidade informático-digital, somos, assim, levados a equacionar como seria possível reverter essa situação, por forma a garantir uma "nova tutela especificamente desenhada" [371] para a realidade digital.

Embora os direitos fundamentais sejam dinâmicos, não havendo necessidade de intervenção legislativa prévia para que possam expandir-se, a verdade é que sempre que em causa esteja o alargamento dos meios de intromissão nos direitos fundamentais para fins de investigação criminal, a utilização de tais meios não se vai tornando legítima à medida do desenvolvimento das novas possibilidades técnicas.[372] Assim, a circunstância de as ações encobertas digitais envolverem, em maior ou menor medida, a restrição de direitos fundamentais evidencia o facto de estarmos perante uma matéria que deverá estar sujeita a

---

Público o ordenamento ou validação da apreensão de comunicações "sem prévio controlo do juiz de instrução criminal", numa verdadeira tentativa de "clarifica[ção] [d]o modelo de apreensão de correio eletrónico e da respetiva validação judicial". Sobre esta questão veja-se a nota publicada na página da Internet da Presidência da República, disponível em: https://www.presidencia.pt/atualidade/toda-a-atualidade/2021/08/presidente-da-republica-promulga-cinco-diplomas-e-envia-outro-para-o-tribunal-constitucional/ [Acesso em 09 de março de 2022]; Juliana Campos alerta para o facto de alguma doutrina considerar que os *e-mails* se encontram ainda integrados no conceito jurídico de comunicações, na medida em que ficando sempre disponíveis no servidor, o seu acesso implicará sempre uma violação do direito à inviolabilidade das telecomunicações *Vide:* JULIANA FILIPA SOUSA CAMPOS, *O Malware… Op. Cit.* Pg. 64, nota de pé de página 174; Sobre esta questão também: MANUEL DA COSTA ANDRADE, *Bruscamente no Verão passado…, Op. Cit.* Pg. 164 e ss;

[370] *Cfr.* SÓNIA FIGALDO, *A utilização de inteligência artificial… Op. Cit*. Pg. 139.

[371] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 242.

[372] *Cfr.* SÓNIA FIGALDO, *A utilização de inteligência artificial… Op. Cit.* Pg. 141.

uma "intransponível exigência de reserva de lei"[373], só podendo a tarefa da tutela jurídica da realidade digital fazer-se através da precedência de uma lei ou de um decreto-lei autorizado pela Assembleia da República que permita a densificação do respetivo regime jurídico (em respeito pelo art. 18º, nº2 e 165º, alínea b), da CRP), sem que seja necessário o recurso a analogias.[374]

De facto, a dimensão do princípio da reserva de lei material revela-se nesta sede imprescindível visto que impõe como condição de legitimação deste método oculto restritivo de direitos fundamentais o crivo da *quality of the law.* Ademais, como evidencia Maria Beatriz Seabra de Brito, o juízo de ponderação que materializa o princípio da proporcionalidade no recurso a este método não se faz sem a existência de um regime processual que defina de forma «*clara, detalhada e precisa*» os seus fundamentos, fins e limites.[375]

Nesta aceção, conforme prossegue Benjamim Silva Rodrigues, todas as Leis devem ter em comum determinadas caraterísticas, não devendo as ações encobertas digitais escapar a essa lógica:

"a) *Clareza suficiente para correcta e rigorosa identificação do bem(ns) jurídicos(s) ou direito(s) fundamental(is) envolvido(s);*

---

[373] Neste sentido: MANUEL DA COSTA ANDRADE, *Métodos ocultos de investigação (Pladoyer para uma teoria geral)* – Que futuro para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português, Coimbra: Coimbra Editora, 2009. Pg. 540.

[374] Assim, como refere, David Silva Ramalho, envolvendo os métodos ocultos uma restrição "*não irrelevante"* de direitos fundamentais do visado e de terceiros que pelos mesmos venham, reflexamente, a ser abrangidos, só desta forma será possível alcançar a legitimidade da medida e a validade da prova através dela obtida – DAVID SILVA RAMALHO, *Métodos ocultos … Op. Cit.* Pg. 220; De notar que, como acentua Jorge Novais, a reserva de lei centra a sua importância na segurança jurídica que fomenta nos cidadãos: "os direitos e deveres dos particulares ficam precisamente delimitados na medida em que as possibilidades, modalidades e limites das intervenções estatais concretas que os afectem sejam prévia e suficientemente determinadas e, em princípio, por um órgão que não se encarrega, ele próprio, da aplicação das respectivas normas (…) Por último, a prévia fixação dos critérios a que deve obedecer a futura acção administrativa é condição necessária da tutela efectiva e constitucionalmente adequada dos direitos dos cidadãos, já que, fornecendo ao poder judicial os necessários parâmetros de controlo da actuação administrativa, permite uma tutela jurisdicional plena e conforme aos limites funcionais de cada um poderes." *Cfr.* JORGE NOVAIS, "*As restrições aos Direitos Fundamentais não expressamente autorizados pela Constituição"*, 2ª Ed., Coimbra: Coimbra Editora, 2010. Pg. 832 e ss.; Idêntico pensamento apresenta Juliana Campos na análise da regulação do *malware,* para a qual defendeu a necessidade de a medida da sua utilização ter de estar prevista na lei e de forma autonomizada, isto é, numa norma distinta das dos restantes meios de obtenção de prova que já encontram consagração na lei processual penal. - *Cfr.* JULIANA FILIPA SOUSA CAMPOS, *"O Malware …" Op. Cit.* Pg. 157. Do mesmo modo, JOÃO CONDE CORREIA, *Prova digital… Op. Cit.* Pg. 30.

[375] MARIA BEATRIZ SEABRA DE BRITO, *Novas tecnologias e legalidade da prova em processo penal – natureza e enquadramento do GPS como método de obtenção de prova*, Coimbra: Edições Almedina. 2018. Pg. 102.

b) Correcta definição dos níveis de sacrifício a impor ao bem(s) jurídico(s) ou direito(s) fundamental(is) envolvido(s);

c) Previsão da forma ou modalidade de técnica invasiva usada (ou a utilizar);

d) Previsão e prescrição precisa e clara do fundamento, fim e limites da intromissão – princípio da vinculação do fim (da recolha da informação).”[376]

Assim, enveredar por uma Lei construída nestes moldes seria permitir o conhecimento pelo visado da delimitação da margem de livre atuação das autoridades públicas e do cumprimento dos pressupostos objetivamente verificáveis, concedendo-lhe, dessa forma, a possibilidade de sindicar a legalidade e constitucionalidade de qualquer procedimento de produção de prova, em nome da necessária segurança jurídica.[377]

O estudo que fizemos permitiu-nos concluir que a regulação das atividades do agente encoberto digital por mera remissão legislativa para o RJAE, pensado para atender às especificidades de uma realidade predominantemente física, e para o art. 19º, nº2 da LC, uma extensão daquele que se revela algo vaga e imprecisa, já não se mostra satisfatória. E não só é insatisfatória como é manifestamente desajustada. Deste modo, embora David Silva Ramalho não seja adepto da necessidade de criação de uma nova norma legal habilitante das ações encobertas digitais, porquanto, na sua ótica, traduzem-se na execução de um método oculto já previsto, mas através de um modo diferente, reconhece que “a subsunção de outros meios, por via judicial, aos regimes consagrados para outros métodos ocultos, implica uma ilegítima substituição do aplicador do Direito ao legislador, através da qual afere da similitude de pressupostos e encaixa neles novos métodos para os quais não foram pensados e cuja execução não foi de ponderação legislativa específica”[378].

De facto, a solução de remissão das novas realidades digitais para os velhos modos de aquisição probatória processual penal é geradora de problemas. A ausência de uma reconfiguração das construções jurídico-dogmáticas, dirigidas a novas formas de invasividade ocultas, é responsável, pelo menos em parte, pelas assimetrias e descontinuidades do sistema atual.[379] Nesta medida, como avança Duarte Rodrigues Nunes,

---

[376] BENJAMIM SILVA RODRIGUES, *Da Prova Penal: Novos Métodos “Científicos”… Op. Cit.* Pg. 64 e 65; *Idem,* “*Da Prova Penal: Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos…” Op. Cit.* Pg. 53

[377] *Cfr.* DAVID SILVA RAMALHO, *Métodos ocultos…Op. Cit.* Pg. 221.

[378] *Ibidem.* Pg. 222.

[379] MARIA BEATRIZ SEABRA DE BRITO, *Novas tecnologias e legalidade da prova em processo penal… Op. Cit.* Pg. 100 e 101.

uma regulamentação autónoma justificar-se-ia em face das diferenças evidentes entre a realidade física e a realidade digital, que fazem com que a aplicação à realidade digital de meios de obtenção de prova delineados para a realidade física seja muito difícil e, para ultrapassar essa dificuldade, se recorra a "soluções casuísticas potencialmente inseguras e inadequadas."[380]

Assim, naquela linha de pensamento, entendemos que a regulação das ações encobertas digitais – hoje dispersa e incongruente – deverá ser feita através de uma lei própria, expressa e determinada, em nome do princípio da precisão dos atos normativos, o que poderá ser almejado através da sua inserção num novo capítulo no CPP, destinado à normatização da prova digital. De facto, se as apreensões (previstas e reguladas nos artigos 178º a 186º do capítulo I do Título III do CPP) e as escutas telefónicas (previstas e reguladas nos artigos 187º a 190º do mesmo capítulo) – também métodos de investigação criminal mais invasivos – mereceram consagração no CPP, muito em função do facto de se terem relevado necessários e aptos a dar resposta às especificidades da criminalidade atual, não vemos hoje fundamento para uma tal possibilidade ser negada às ações encobertas.[381]

Ultrapassado o problema da habilitação legal específica para o recurso a este método oculto de investigação criminal, passar-se-ia para o plano da densidade normativa da lei habilitante, isto é, do conteúdo e da extensão da medida restritiva de direitos fundamentais,[382] em consonância pelo exigido pelos princípios da proibição do excesso, da igualdade e da proteção da confiança.[383] Assim, daquela consagração seria possível adensar-se determinados aspetos materiais que as ações encobertas digitais carecem ainda de regulação, sobretudo os relacionados com as condições e os limites da sua utilização[384],

---

[380] DUARTE ALBERTO RODRIGUES NUNES, *Os meios de obtenção… Op. Cit.* Pg. 203.
[381] Neste sentido parece dirigir-se Armando Dias Ramos, na medida em que, segundo o Autor, "a utilização do agente encoberto digital será a breve trecho, como o foi há uns anos as escutas a telemóveis, uma forma inquestionável das autoridades judiciárias obterem elementos de prova do mundo digital, quando os demais meios forem impossíveis." *Cfr.* ARMANDO DIAS RAMOS, *O agente encoberto digital… Op. Cit.* Pg. 286. Também a favor desta possibilidade de inserção no próprio CPP de um regime geral de obtenção de prova eletrónica, onde naturalmente se incluiriam as ações encobertas digitais, parece manifestar-se Paulo Dá Mesquita, apontando uma série de argumentos capazes de afastar as três ordens de razões apresentadas na exposição de motivos da proposta da Lei do Cibercrime para o enquadramento sistemático que foi adotado, razões essas que se revelam, no seu entender, "frágeis na sustentação exposta, contraditórias em si mesmas e incompatíveis com o regime introduzido". *Vide:* PAULO DÁ MESQUITA, *Processo Penal… Op. Cit.* Pg. 98 e 99.
[382] DAVID SILVA RAMALHO, *Métodos ocultos… Op. Cit.* Pg. 223.
[383] Sobre essas exigências veja-se, mais desenvolvidamente: JORGE NOVAIS, *As restrições aos Direitos… Op. Cit.* Pgs. 727 a 820.
[384] Que fomos já concretizando ao longo do presente capítulo.

consoante o nível de ingerência nos direitos, liberdades e garantias que cada concreta atuação do agente encoberto digital reclama, tais como:

1. A corporização no texto da Lei de uma noção de agente encoberto digital, podendo ser definido como o funcionário público ou terceiro particular que, voluntariamente e por decisão de uma autoridade judicial, se infiltra em meios virtuais, com recurso a aparelhos e dispositivos informáticos, com o objetivo de obter informações sobre os autores e respetivos modos de atuação em certas práticas ilícitas no mundo virtual (e, dessa forma, recolher eventual prova incriminatória);
2. A consagração da impossibilidade expressa de um terceiro (co)arguido encetar, ele próprio, a ação encoberta digital, podendo apenas, no limite, intervir na investigação de forma indireta/passiva, através, por exemplo, da cedência aos OPC das suas credenciais de acesso aos canais de comunicação; ou, em última instância, caso a sua intervenção ativa se revele efetivamente necessária, serem definidas pelos OPC as regras a que deve obedecer na sua atuação, ficando sujeita a um minucioso controlo judicial;
3. A admissibilidade em termos excecionais da utilização de Cybercops criados por terceiros; a serem utilizados, apenas deverão poder ser monitorizados junto dos OPC competentes e depois de obtida a respetiva autorização judicial;
4. A enunciação expressa dos critérios de seleção e de escolha dos agentes encobertos digitais no texto da Lei (*v.g.* qualidades psicológicas, conhecimentos informático-digitais e "pegada digital");
5. A previsão de um catálogo de crimes com uma amplitude razoável do ponto de vista jurídico-constitucional, ficando as ações encobertas digitais cingidas aos tipos de crime de natureza mais gravosa, em função das exigências dos princípios da proporcionalidade e da necessidade;
6. A concretização do conceito de "meios e dispositivos informáticos" passíveis de serem utilizados no âmbito das investigações em ambiente digital, capaz de afastar as inúmeras e distintas interpretações que têm sido feitas. Dessa concretização poderia resultar, eventualmente, a legitimação do envio de *benware* e a definição dos seus termos de utilização;

7. A previsão dos termos e modo da possibilidade de cumulação de ações encobertas digitais com outros métodos ocultos de obtenção de prova;
8. A consagração expressa da possibilidade de prossecução de finalidades preventivas no âmbito das ações encobertas digitais, em casos devidamente sinalizados, justificados e de especial complexidade de investigação;
9. A previsão da possibilidade de, em determinados casos, ser valorada prova que tenha sido obtida em momento anterior à emanação da respetiva autorização judicial habilitante, desde que posteriormente validada pelo JIC. Obtida que tenha sido a referida autorização judicial habilitante, do despacho devem constar alguns pormenores subjacentes à investigação, via esclarecedora da validade quer de atos praticados em momento anterior à obtenção da autorização, quer de atos posteriores, tais como: quais os utilizadores dos canais de comunicação cuja investigação é admitida, quais os sistemas informáticos a partir dos quais são permitidas as atividades investigativas, quais os atos autorizados e não autorizados (para evitar quaisquer tipos de abusos) e ainda quais os *websites*, *chats* ou fóruns (ou outro tipo de canais) autorizados a frequentar, bem como com quem é legítimo interagir e estabelecer contactos mais intensos e duradouros.
10. A densificação do conceito de "identidade fictícia" à luz da concreta natureza das ações encobertas em ambiente informático-digital, bem como da extensão da sua putativa atribuição e utilização;
11. A consagração do princípio-regra da junção do relato do agente encoberto ao processo, onde sejam discriminados os traços gerais da sua operação.
12. A imposição de àquele relato serem juntos registos efetuados pelo agente, anexados com uma periodicidade de 15 em 15 dias (ou, no limite, de 30 em 30 dias), e onde sejam descritos determinados pormenores que remontem a específicos momentos da investigação;
13. A introdução da diferenciação entre as operações que decorrem em canais «abertos» das que decorrem em canais «fechados» de comunicação, com a enunciação das situações em que o agente necessita de estar efetivamente munido de uma prévia autorização judicial para poder atuar.
14. A clarificação dos limites da desresponsabilização criminal pelos atos ilícitos eventualmente praticados pelo agente no exercício das suas atividades

investigativas, bem como do que sucederá à prova que, embora dotada de qualidade probatória, tenha sido alcançada em moldes manifestamente abusivos, isto é, fora dos termos autorizados.

De relevar, porém, que a previsão de uma Lei habilitante com a fixação da sua compreensão, extensão, vinculação finalístico-teleológica e dos seus limites, conforme defende Costa Andrade[385], não deverá motivar o aniquilamento do espaço de discricionariedade da atuação judicial para a necessária adaptação das regras processuais aos casos concretos.

Por conseguinte, como defende David Silva Ramalho, como forma de se obstar à aplicação fria das normas, o legislador poderá socorrer-se de fórmulas como "*se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter",* conforme já o faz no art. 187º do CPP[386], a partir das quais se poderá legitimar juízos casuísticos, operados dentro do exigido pelo princípio da proporcionalidade, verdadeiramente capazes de evitar que a "regulamentação [seja] tão estrita e minuciosa ao ponto de petrificar a actuação judicial".[387]

Expostos estes termos e seguidas que fossem estas orientações, cremos que estariam criadas as condições necessárias à mudança no modo como este método de obtenção de prova é reputado no seio do processo penal, apartando-o do domínio estrito da analogia com o mundo físico e dando-lhe espaço para crescer de forma livre, autónoma e autossuficiente.

[385] MANUEL DA COSTA ANDRADE, *Métodos ocultos de investigação (Pladoyer para uma teoria geral)… Op. Cit.* Pg. 541.
[386] *Cfr.* DAVID SILVA RAMALHO, *Métodos ocultos … Op. Cit*. Pg. 229.
[387] *Ibidem.* Pg. 225.

BIBLIOGRAFIA

— ALVES DE SOUSA, Maria Clara de Freitas Morna, *O Agente Infiltrado No Ordenamento Jurídico Português,* Dissertação de Mestrado, Faculdade Direito da Universidade Coimbra, Coimbra, 2012.

— AIRES DE SOUSA, Susana, *Agent Provocateur e meios enganosos de prova. Algumas reflexões, in* Separata de Liber Discipulorum para Jorge de Figueiredo Dias." Coimbra: Coimbra Editora, 2003.

- *Ações encobertas (e outras figuras próximas) na investigação da criminalidade económico-financeira in* Revista Julgar nº 38, maio/agosto de 2019.

— ANDRADE, Manuel da Costa, *Anotação ao Acórdão nº 364/2006, de 8 de junho (Domicílio, Intimidade e Constituição),* RLJ, ano 138º, nº 3953, novembro/dezembro de 2008.

- *Bruscamente no verão passado: a reforma do Código de Processo Penal: observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora, 2009.
- *Métodos ocultos de investigação (Pladoyer para uma teoria geral)* – Que futuro para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português, Coimbra: Coimbra Editora, 2009.
- *Comentário ao art. 190º in* Comentário Conimbricense do Código Penal: Parte Especial (dir. Jorge Figueiredo Dias), Tomo I, 2ª Edição, Coimbra: Coimbra Editora, 2012.
- *Anotação ao artigo 194º do CP – Violação de correspondência ou de telecomunicações, in* Comentário Conimbricense do Código Penal, Tomo I, 2ª Edição, 2012.
- *Sobre as Proibições de Prova em Processo Penal*, Coimbra: Coimbra Editora, 2013.

— ANTUNES, Maria João, *Direito ao silêncio e leitura em audiência de declarações do arguido*, in SubJudice, Justiça e Sociedade, n. º4, setembro/dezembro 1992.

— BUENO DE MATA, Federico, *El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia*, *in* Actas del IV Congreso Galego de Derecho Procesal (I internacional), A Coruña, 117 2 y 3 de junio de 2011.

— CANOTILHO, J.J./ MOREIRA, Vital, *Anotação ao art. 26º* in Constituição da República Portuguesa Anotada, vol. I, 4ª Ed. Revista, Coimbra: Coimbra Editora, 2007.

- *Anotação ao art. 34º in* Constituição da República Portuguesa Anotada, vol. I, 4ª Ed. Revista, Coimbra: Coimbra Editora, 2007.

— CAMPOS, Juliana Filipa Sousa, *O Malware como Meio de Obtenção de Prova em Processo Penal*, Coimbra: Edições Almedina, 2021.

— CONDE CORREIA, João, *Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art.º 32.º, n.º 8, 2ª parte, da C.R.P.) in* Revista do Ministério Público, ano 20.º, n.º 79, 1999.

— DEPARTMENT OF JUSTICE, *Online Investigative Principles for Federal Law Enforcement Agents*, 1999. Disponível em: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf [Acesso em: 14 de dezembro de 2021].

— DIAS RAMOS, Armando, *O agente encoberto digital: meios especiais e técnicos de investigação criminal*, Coimbra: Edições Almedina, 2022.

- *A investigação do Cibercrime – Nótulas sobre o paradigma legislativo atual e a realidade tecnológica in Cyberlaw by CIJIC,* Edição nº VIII, setembro de 2019.
- *A prova digital em processo penal: o correio eletrónico*, 2ª Edição atualizada e ampliada, Lisboa: Chiado Editora, 2014.

— DIAS VENÂNCIO, Pedro, *Lei do Cibercrime Anotada e Comentada* [Art. 19º]. Coimbra: Coimbra Editora, 1ª Edição, janeiro de 2011.

— FIGALDO, Sónia, *Determinação do perfil genético como meio de prova em processo penal*, in Revista Portuguesa de Ciência Criminal, janeiro-março de 2006.

- A *utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo in* A inteligência Artificial no Direito Penal [Coord: Anabela Miranda Rodrigues], Coimbra: Edições Almedina, 2020.

— FIGUEIREDO DIAS, Jorge de, *Sobre os Sujeitos Processuais no Novo Código de Processo Penal, in* Jornadas de Direito Processual Penal, O Novo Código de Processo Penal, Centro de Estudos Judiciários, Coimbra: Almedina, 1991.

- *Direito Penal: Parte Geral, Tomo I: Questões Fundamentais, A Doutrina Geral do Crime,* 3ª Edição, Coimbra: Gestlegal, 2020.

— FIGUEIREDO DIAS, Jorge/ COSTA ANDRADE, Manuel da, *(Parecer) in Supervisão, Direito ao silêncio e legalidade da prova* (CMVM), Coimbra: Almedina, 2009.

— FILHO, Nivaldo Machado, *O Agente Infiltrado em duelo com o contraditório: aspectos críticos de seu relatório e depoimento* in Revista de Concorrência e Regulação, Ano VIII. Número 31, julho/setembro de 2017.

— FONSECA, J. Martins*, O Conceito de Domicílio, face ao Art. 34º da Constituição da República, in* Revista do Ministério Público, nº 45, ano 12º, 1991.

— FREITAS, José Pedro, *Os meios de obtenção de prova digital na investigação criminal. O regime jurídico dos serviços de correio eletrónico e de mensagens curtas*, Braga: Nova Causa Edições Jurídicas, 2020.

— GODINHO, Jorge Alexandra Fernandes, *Do crime de "branqueamento de capitais*: Introdução e Tipicidade, Edições Almedina, 2001.

— GONÇALVES, Fernando/ ALVES, Manuel João/ VALENTE, Manuel Monteiro Guedes, O *novo regime jurídico do agente infiltrado: Comentado e Anotado - Legislação Complementar.* Coimbra: Editora Almedina, 2001.

- *Lei e Crime: O agente infiltrado versus o agente provocador. Os princípios do processo penal.* Coimbra: Almedina, 2001.

— GONÇALVES, Fernando/ ALVES, João Manuel, *Crime. Medidas de Coação e Prova. O agente infiltrado, encoberto e provocador,* Coimbra: Edições Almedina, 2015.

— Guia Legislativo para a Aplicação da Convenção nas Nações Unidas contra a criminalidade Organizada Transnacional. Ministério da Justiça. Vancouver, março de 2003.

— KARL-HEINZ, Gössel, *As proibições de prova no direito processual penal in* Revista Portuguesa de Ciência Criminal, julho-setembro de 1992.

— LORCA SÁNCHEZ, Miguel Ángel, *El derecho al secreto de las comunicaciones. Influencia de la jurisprudencia y análisis de su aplicación en la práctica jurídica.* Tesis Doctoral, Universitat d' Alacant, Facultad de Derecho, Departamento Derecho Mercantil y Derecho Procesal, Enero 2021.

— MAGLIE, Cristina de, *L'Agente Provocatore – Un'indagine dommatica e politicocriminale*, Milano: Milano - Dott. A. Giuffrè Editore, 1991.

— MARQUES DA SILVA, Germano, *Bufos, infiltrados e arrependidos. Os princípios Democrático e da Lealdade em processo penal in* Direito e Justiça, Revista da Faculdade de Direito da Universidade Católica, Vol. VIII, II, 1994.

- *Direito Processual Penal Português. Noções e princípios gerais, sujeitos processuais, responsabilidade civil conexa com a criminal, objeto do processo.* Vol. I.. Lisboa: Universidade Católica Editora, 2017.
- *Curso de Processo Penal* – Vol. II, 5ª Edição, revista e actualizada. Lisboa: Edição Babel, 2011.

— MATA-MOUROS, Fátima, *Infiltrados fora da lei, Sub Judice – justiça e sociedade*, Coimbra, nº 18, 2000.

— MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas pelo Agente Provocador em Processo Penal*, Coimbra: Almedina, 1999.
- *Homens de confiança* in II Congresso de Processo Penal, Lisboa: Almedina, 2006.

— MESQUITA, Paulo Dá, *Processo Penal, prova e sistema judiciário,* Coimbra: Coimbra Editora. 1ª Edição, setembro de 2010.
- *A Prova do Crime e o que se disse Antes do Julgamento – Estudo sobre a Prova no Processo Penal Português, à Luz do Sistema Norte-Americano,* Coimbra: Coimbra Editora, 2011.

— MONTE, Mário Ferreira, *Anotação ao relatório da Comissão Europeia dos Direitos do Homem, Processo nº 25829/94, Francisco Teixeira Castro contra Portugal in* Scientia Iuridica – Revista de direito comparado português e brasileiro. T. XLVI. Universidade do Minho, 1997.

— MONTEIRO GUEDES VALENTE, Manuel, *Processo Penal, Tomo I*, 2010.

— MONIZ, Helena, *Notas sobre a protecção de dados pessoais perante a informática in* Revista Portuguesa de Ciência Criminal, abril-junho de 1997.

— NEVES, Rita Castanheira, *As ingerências nas Comunicações Electrónicas em Processo Penal, Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, 1ª Edição, Coimbra: Coimbra Editora, 2011.

— NOVAIS, Jorge Novais, *As restrições aos Direitos Fundamentais não expressamente autorizados pela Constituição*, 2ª Edição, Coimbra: Coimbra Editora, 2010.

— NUNES, Duarte Alberto Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Coimbra: Gestlegal, 1ª Edição, abril 2018.

- *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada,* 1ª Edição, Coimbra: GESTLEGAL, 2019.
- *O agente infiltrado online no direito português, in:* Revista Ultracontinental de Literatura Jurídica, Ed. Associação de Letras Jurídicas de Montes Claros, Montes Claros, v. 2, n. 3, set.-dez. 2021.

— OLIVEIRA E SILVA, Sandra, *A proteção de testemunhas no processo penal*, Coimbra: Coimbra Editora, 2007.

- *Salas vazias e declarações anónimas. Notas sobre a proteção de testemunhas e o processo equitativo no julgamento da criminalidade organizada in* Revista do CEJ, Dossiê Temático Criminalidade Económico-Financeira e Criminalidade Organizada. 2º Semestre 2011, nº 16.
- *O Arguido como Meio de Prova contra si mesmo: Considerações em torno do princípio nemo tenetur se ipsum accusare*. Coimbra: Editora Almedina, 2019 (Reimpressão).

— ONETO, Isabel, *O Agente Infiltrado: Contributo para a compreensão do regime jurídico das ações encobertas.* Coimbra: Coimbra Editora, 2005.

— PANDA SECURITY, *El mercado negro del Cibercrimen al descubierto*. Disponível em: https://www.pandasecurity.com/es/mediacenter/src/uploads/2014/07/Mercado-Negro-del-Cybercrimen.pdf [Acesso em 11 de novembro de 2021).

— PAIVA, Vitor, *Agente infiltrado, no âmbito de ação encoberta, in* Revista do Ministério Público. ISSN 0870-6107. A. 35, nº 137, 2014.

— PELLUCCI, Frederico, *A atuação dos Agentes Encobertos e Infiltrados nos Canais Abertos e Fechados de Comunicação em Ambiente Informático-Digital in* Novos Desafios da Prova Penal, Coordenação Paulo de Sousa Mendes e Rui Soares Pereira, Almedina, 2020.

— PEREIRA, Sandra, *A recolha de prova por agente infiltrado*, in Prova Criminal e Direito de Defesa: Estudos sobre teoria da prova e garantias de defesa em processo penal. Ana Rita Fidalgo.. [et al.] / coordenação [de] Teresa Pizarro Beleza, Frederico de Lacerda da Costa Pinto. Coimbra: Editora Almedina, 2010.

— PINTO DE ALBUQUERQUE, Paulo, *Comentário ao código de processo penal à luz da constituição da República e da Convenção Europeia dos Direitos do Homem.* 4. Edição, Lisboa: Ed. Universidade Católica, 2011.

- *Comentário do Código de Processo Penal*, 4.ª Edição atualizada, Lisboa: Universidade Católica Editora, 2018.
- *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2ª Edição, Universidade Católica Editora, Lisboa, 2008.

— PINTO DE SOUSA, Paulo, *Acções Encobertas. Meio enganoso de prova? Agente infiltrado e agente provocador. Outras questões* in Revista do CEJ, Editora Almedina, 2010.

— RAMALHO, David Silva, *O uso de malware como meio de obtenção de prova em processo penal in:* Revista de concorrência e regulação - C&R. ISSN 1647-5801. Ano 4, n.º 16, 2013.
    - *A investigação criminal na Dark Web, in* Revista da Concorrência & Regulação, ano IV, nº 14/15 (abril/setembro), 2013.
    - *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra: Edições Almedina, 2019.

— RODRIGUES, Benjamim Silva, *Da Prova Penal*: *Novos Métodos "Científicos" de Investigação Criminal nas Fronteiras das Nossas Crenças*, Tomo VI, 1ª Edição, Lisboa: Rei dos Livros, 2011.
    - *Da Prova Penal: Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, Tomo II, 1ª Edição, Lisboa: Rei dos Livros, 2010.

— SEABRA DE BRITO, Maria Beatriz, *Novas tecnologias e legalidade da prova em processo penal – natureza e enquadramento do GPS como método de obtenção de prova*, Coimbra: Edições Almedina, 2018.

— STANGHERLIN, Marina, AUGUSTO PETEAN, Fabiano, *Agente Infiltrado – Sua natureza jurídica na produção digital de provas,* 1ª Edição, Editora Appris, ISBN: 978-65-250-0902-5, 2021.

— TEMPERINI, Marcelo/ MACEDO, Maximiliano, *Nuevas Herramientas de Investigación penal: el agente encubierto digital in* "*Cibercrimen: aspectos de derecho penal y procesal penal: cooperación internacional: recolección de evidencia digital: responsabilidad de los proveedores de servicios de internet*", Montevideo Buenos Aires, 2016.

— VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial,* 2.ª Edição, Coimbra: Almedina, 2009.

— VIEIRA DE ANDRADE, José Carlos *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 6ª Edição, Coimbra: Almedina, 2019.

— ZARAGOZA TEJADA, Javier, *El Agente Encubierto "online" in* Investigación tecnológica y derechos fundamentales: comentarios a las modificaciones introducidas por la ley 13/2015, ARANZADI / CIVITAS, 2017.

LEGISLAÇÃO

Constituição da República Portuguesa

Código Penal (DL n.º 48/95, de 15 de Março)

Código Processo Penal (DL n.º 78/87)

Regime Jurídico das Ações Encobertas (Lei nº 101/2001 de 25 de agosto)

Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro)

Lei de Organizações Criminosas (Lei 12.850/13)

Ley de Enjuiciamiento Criminal

JURISPRUDÊNCIA

Acórdão do TC nº 58/98 de 14 de outubro. Disponível em: http://www.pgdlisboa.pt/jurel/cst_main.php?ficha=9321&pagina=310&nid=3845

Acórdão do TC nº 364/2006 de 8 de junho. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20060364.html

Acórdão do STJ de 10 de março de 2016. Disponível em: Acórdão do Supremo Tribunal de Justiça (dgsi.pt)

STS 1385/2018 de 11 de abril. Disponível em: https://www.poderjudicial.es/search/documento/TS/8370270/abusos%20sexuales/20180504 [Acesso em: 11 de janeiro de 2022].

STS 752/2010, de 14 de julho. Disponível em: https://vlex.es/vid/-218422135 [Último acesso em: 04 de março de 2022].

STS 767/2007, de 3 de outubro. Disponível em: https://vlex.es/vid/facilitacion-pornografia-infantil-p-31969904 [Acesso em: 18 de maio de 2022].

Acórdão do Tribunal Distrital dos Estados Unidos, SD Ohio, Divisão Leste de 30 de setembro de 1997. Case of *United States v. Charbonneau* Disponível em: https://law.justia.com/cases/federal/district-courts/FSupp/979/1177/1446971/ [Acesso em: 01 de abril de 2022].

BverfG, 1 BvR 370, 595/07, disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html

SITES

https://www.presidencia.pt/atualidade/toda-a-atualidade/2021/08/presidente-da-republica-promulga-cinco-diplomas-e-envia-outro-para-o-tribunal-constitucional/ [Acesso em: 09 de março de 2022].

https://expresso.pt/sociedade/2022-03-15-Esta-na-altura-de-criar-uma-lei-para-agentes-infiltrados-do-cibercrime-defende-presidente-de-Observatorio-de-Terrorismo-dcb13996 [Acesso em: 22 de março de 2022].

https://desporto.sapo.pt/futebol/artigos/entenda-o-caso-football-leaks-e-o-papel-do-portugues-rui-pinto-2 [Acesso em: 20 de abril de 2022].