UNIVERSIDADE D
COIMBRA

Ana Rita Almeida Guedes

O Agente Encoberto Digital enquanto Método Oculto de Obtenção de Prova

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

Outubro de 2021

Ana Rita Almeida Guedes

O Agente Encoberto Digital enquanto Método Oculto de Obtenção de Prova

The digital undercover agent as a hidden method of obtaining evidence

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

Coimbra, 2021

AGRADECIMENTOS

Em primeiro e como sempre em tudo o que faço: aos meus pais e irmã. Todas as minhas vitórias a vós vos devo e são totalmente vossas. Por toda a confiança, amor incondicional e compreensão que sinto sempre o meu Obrigada.

À Faculdade de Direito da Universidade de Coimbra que, além dos ensinamentos no mundo do Direito, ensinou-me a nunca desistir, a lutar e a acreditar sempre em mim.

À minha orientadora, a Doutora Susana Aires de Sousa. Senti sempre o acompanhamento e apoio esperados nesta época. Por todas as sugestões e disponibilidade, o meu sincero agradecimento.

A Coimbra que tanto me deu e ensinou e a todas as amizades que fiz nesta Cidade incrível. Todos contribuíram para chegar aqui. Não consigo dizer o quão feliz fui. Levo as melhores memórias e ficam todos comigo no meu coração.

A todos os que foram compreensivos e encorajadores nesta etapa e me ajudaram a que este trabalho fosse concluído. Obrigada.

RESUMO

Os novos desenvolvimentos tecnológicos observados no último século afiguram-se bastante úteis para nós enquanto sociedade descomplicando a nossa vida em várias vertentes e aproximando-nos das diferentes partes do globo muito rapidamente. Por outro lado, tais inovações trazem consigo uma nova criminalidade à qual o Direito não pode ser alheio. Assim, tendo em conta este novo mundo que se vai formando, o Direito tem que ser capaz de dar uma resposta cabal e completa, não podendo ficar inerte.

Iremos, nesta dissertação, atentar no caso específico das Ações Encobertas em Ambiente Digital admitidas pelo art. 19.º da Lei n.º 109/2009 de 15 de setembro (Lei do Cibercrime). O uso de agente encoberto em ambiente digital, enquanto um método oculto de obtenção de prova, tem como objetivo a descoberta da verdade material. Contudo, neste percurso, direitos fundamentais poderão ser lesados. Será que esta verdade material pode ser admitida a todo custo e a todo o preço[1]? Será que se afigura razoável a aplicação do RJAE, uma legislação de 2001 pensada para o mundo físico, às ações encobertas desenvolvidas em ambiente digital? Deveria ter sido outra a solução do legislador? Serão algumas das questões que pretendemos ver respondidas no fim desta dissertação.

Começaremos o nosso itinerário abordando as Ações Encobertas e o disposto na Lei n.º 101/2001 de 25 de agosto. No capítulo seguinte, analisaremos as especificidades que o ambiente digital convoca e a utilização do agente encoberto como método de obtenção de prova. Por fim, atentaremos na temática da Prova Digital e das Buscas *online*.

Palavras-Chave: Ações Encobertas; Agente Encoberto Digital; Métodos Ocultos; Prova Digital; Buscas *Online*

[1] JORGE FIGUEIREDO DIAS, *Direito Processual Penal: Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por Maria João Antunes*, 1998-1989 , p. 22; MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova em processo penal*, 2013, p.117

ABSTRACT

The new technological developments observed in the last century appear to be quite useful for us as a society, making our lives uncomplicated in various aspects and approaching different parts of the globe very quickly. On the other hand, such innovations bring a new criminality to which the Law cannot be oblivious. Thus, taking into account this new world that is being formed, the Law needs to be able to provide a full and complete answer, and cannot be inert.

We will, in this dissertation, pay attention to the specific case of Undercover Actions in Digital Environment admitted by the art. 19 of Law no. 109/2009 of September 15th (Cybercrime Law). The use of an undercover agent in a digital environment, as a hidden method of obtaining evidence, aims to discover the material truth. However, on this path, fundamental rights are compromised. Can this material truth be admitted at all costs? Does it seem reasonable to apply RJAE (Law no. 101/2001, August 25th), a 2001 legislation designed for the physical world, to undercover actions developed in a digital environment? Should the legislator's solution have been different? These will be some of the questions we intend to see answered at the end of this dissertation.

We will start our itinerary by addressing the Undercover Actions and the provisions of Law No. 101/2001 of August 25th. In the next chapter, we analyze the specificities that the digital environment calls for and the use of the undercover agent as a method of obtaining evidence. Finally, we will pay attention to the Digital Evidence and online search.

Keywords: Undercover Actions; Digital Undercover Agent; Hidden Methods; Digital Evidence; Online Searches

SIGLAS E ABREVIATURAS

Ac./Acs. Acórdão/Acórdãos
AE Agente Encoberto/Ações Encobertas
Al. Alínea
Apud Citado por
Art./Arts Artigo/Artigos
CC Código Civil
CCiber Convenção sobre o Cibercrime
CEDH Convenção Europeia dos Direitos do Homem
Cf. Confira/Confronte
CP Código Penal
CPP Código de Processo Penal
CRP Constituição da República Portuguesa
DF's Direitos Fundamentais
DL Decreto-Lei
DLG's Direitos Liberdades e Garantias
Ibid. Ibidem
JIC Juiz de Instrução Criminal
LC Lei do Cibercrime
LCI Lei da Criminalidade Informática
MP Ministério Público
Nº/Nºs Número/Números
Ob. cit. Obra citada
OJ Ordenamento Jurídico
OPC Órgão de Polícia Criminal
P./PP. Página/Páginas
PJ Polícia Judiciária
PSP Polícia de Segurança Pública
RJAE Regime Jurídico das Ações Encobertas
RMP Revista do Ministério Público
ROA Revista da Ordem dos Advogados

STJ Supremo Tribunal de Justiça

TC Tribunal Constitucional

TEDH Tribunal Europeu dos Direitos do Homem

TRE Tribunal da Relação de Évora

TRL Tribunal da Relação de Lisboa

TRP Tribunal da Relação do Porto

V.g. Verbi gratia (por exemplo)

Índice

Introdução e Enquadramento

A autêntica revolução digital que vivemos traz consigo novos desafios para a investigação criminal. Assim, somos confrontados com um novo universo criminal ao qual os métodos de investigação tradicionais não conseguem dar resposta.

Para fazer face a uma "nova fenomenologia criminal"[2], surge a figura do Agente Encoberto na década de 80 circunscrito ao tráfico de estupefacientes sendo, ao longo dos anos, alargado o seu âmbito. Hoje, temos as Ações Encobertas reguladas na Lei n.º 101/2001 de 25 de agosto estabelecendo-se nesta o seu objeto, âmbito de aplicação, requisitos e outras matérias. Cada um destes aspetos será estudado em pormenor.

Por força da Convenção sobre o Cibercrime do Conselho da Europa, o legislador teve que adaptar o direito interno sendo aprovada a Lei n.º 109/2009 de 15 de setembro (LC). No art. 19.º desta lei procedeu-se a um alargamento do âmbito de aplicação (previsto no art. 2.º do RJAE) das Ações Encobertas. Assim, será possível recorrer a este método oculto de investigação no âmbito da cibercriminalidade, remetendo, este art. 19.º, para o disposto no RJAE. Questionamos se, com este alargamento, as Ações Encobertas em Ambiente Digital são encaradas, pelo legislador, como uma "modalidade ou uma outra vertente da ação encoberta"[3]. Acompanhamos RAMALHO quando este critica a subsunção destas ações no regime geral e quando afirma que tal leva a "soluções casuísticas potencialmente inseguras e inadequadas"[4]. Assume grande relevância a dificuldade de distinção, em ambiente digital, entre AE e agente provocador e o uso de identidade fictícia ao abrigo do art. 5.º do RJAE. De extrema importância será, também, a obtenção de prova por este agente. Atentaremos nas especificidades da prova digital e analisaremos a (in)admissibilidade das buscas *online* e o conflito destas com os direitos fundamentais.

---

[2] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", *A reforma do Código de Processo Penal- Observações críticas de uma lei que podia e devia ter sido diferente*, 2009, p. 106

[3] DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, 2017, p. 284

[4] *Ibid.*

CAPÍTULO I. O Agente Encoberto no Ordenamento Jurídico Português

1. Nota sobre a evolução legislativa da figura

A figura do AE teve a sua primeira referência no Direito Português com o DL n.º 430/83 de 13 de dezembro (Lei da Droga) especificamente no seu art. 52.º cujo conteúdo se resumia ao seguinte: "1 - Não é punível a conduta do funcionário de investigação criminal que, para fins de inquérito preliminar, e sem revelação da sua qualidade e identidade, aceitar diretamente ou por intermédio de um terceiro a entrega de estupefacientes ou substâncias psicotrópicas. 2 - O relato de tais factos será junto ao processo no prazo máximo de 24 horas". Posteriormente, com o DL n.º 15/93 de 22 de janeiro, o conteúdo daquele art. 52.º passa a estar reproduzido no art. 59.º deste diploma. No ano seguinte, com a Lei n.º 36/94 de 29 de setembro permite-se, com o seu art. 6.º, o recurso a esta figura nos crimes de corrupção e criminalidade económico financeira.

Como referido, foram sendo introduzidas ao longo do tempo algumas alterações, até ao Regime que hoje conhecemos. Foi em 2001, com a Lei n.º 101/2001 de 25 de agosto que foi criado o Regime Jurídico das Ações Encobertas revogando expressamente os artigos 59.º e 59.º A do Decreto-lei 15/93 e o artigo 6.º da Lei n.º 36/94 ampliando-se o âmbito de aplicação da utilização do agente infiltrado

2. O Regime Geral das Ações Encobertas: análise crítica

2.1 Artigo 1.º "Objeto"

Não podemos começar a presente dissertação sem elaborar um conceito do que entendemos por AE, o objeto de todo este estudo. No RJAE não encontramos um conceito de agente, mas sim de Ações Encobertas. No n.º2 encontramos a definição destas considerando-se que são ações "desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade". Para melhor

percebermos o que consideramos ser AE, convocamos o conceito de COSTA ANDRADE que o entende como alguém que "ocultando a sua identidade e seus propósitos, se intrometem no ambiente das pessoas a investigar e, depois de ganhar a sua confiança ou até amizade, obtêm delas conhecimentos e provas"[5]. Assim, o AE será um funcionário da investigação criminal, ou terceiro atuando sob o controlo da polícia, que se intromete num ambiente criminoso, ocultando a sua qualidade, com o propósito de recolher provas para a investigação criminal. Para tal, cria laços de confiança e amizade com os criminosos, nunca instigando ou instrumentalizando os suspeitos à prática de ilícitos.

Muitas outras conceções têm sido avançadas pela doutrina. Algumas assentam na distinção entre agente infiltrado e AE. Não seguiremos esse caminho e discordamos dessa necessidade. Acompanhando as palavras de RAMALHO, esta diferenciação revela-se inútil e gera confusão[6].

Devemos também manifestar a nossa discordância quando, na elaboração do conceito de AE, alguns autores o entendem como um mero observador, um agente passivo que apenas assiste ao acontecimento criminoso. Esta conceção é defendida por ALVES MEIREIS que faz uma distinção entre agente infiltrado e AE. Para este, o AE será um funcionário policial ou um terceiro à sua ordem que, sem revelar a sua identidade, frequenta meios previsivelmente criminosos com o objetivo de recolher possíveis indícios relevantes, mas cuja presença e cuja realidade "não determinam nem influenciam de forma alguma o rumo dos acontecimentos, naquele lugar e naquele momento poderia estar qualquer outra pessoa e as coisas aconteceriam da mesma forma"[7] . No que concerne ao agente infiltrado, o autor diz-nos que este se mantém a par dos acontecimentos criminosos, acompanhando-os e praticando atos de execução se tal se revelar necessário. Assim, segundo o autor, a principal diferença entre agente infiltrado e AE assenta no grau de intervenção e de integração na situação criminosa. Enquanto o encoberto é um mero observador caraterizado pela sua

[5] MANUEL DA COSTA ANDRADE, "Métodos Ocultos de Investigação Criminal: plädoyer para uma teoria geral", in *Que futuro para o direito* processual penal? *Simpósio em homenagem a Jorge Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português (coord. Mário Ferreira Monte)*, 2009, p. 534
[6] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., pp. 289-290
[7] MANUEL AUGUSTO ALVES MEIREIS, "Homens de confiança" - Será o caminho? *in II Congresso de Processo Penal* (coord.: Manuel Monteiro Guedes Valente), 2006, p. 93

"absoluta passividade relativamente à decisão criminosa"[8], o infiltrado toma parte na execução do acontecimento criminoso.

Parece-nos, acompanhando ONETO, que esta figura de AE descrita por ALVES MEIREIS se enquadra na figura do "agente à paisana".[9] Como tal, sobre este, recai, por exemplo, a obrigação de deter quem seja apanhado em flagrante delito (Cf: alínea a) do n.º1 do art 255.º do CPP). Por outras palavras, este agente à paisana só não é de imediato identificado como agente da autoridade porque não se encontra fardado.

Feitas as considerações sobre o que consideramos ser o AE, passaremos a analisar as Ações Encobertas em si.

Em primeiro lugar, o RJAE tem como finalidade a prevenção e investigação criminal (n.º1 do art. 1.º RJAE). As ações com fins preventivos, em palavras simplistas, terão como função a recolha de informações de forma a evitar a prática de factos ilícitos. Segundo o n.º2 do art. 272.º da CRP, cabe à PJ esta função de prevenção dos crimes, sendo estabelecido no n.º1 do mesmo artigo um limite a esta atuação que se traduz no respeito pelos DLG's dos cidadãos. Já no que concerne à investigação criminal socorremo-nos do conceito plasmado na Lei n.º 49/2008 de 27 de agosto que, no seu art. 1.º, define a investigação criminal como o "conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo."

Ainda neste âmbito, é referido no n.º2 do art. 1.º que a atuação do AE tem como escopo a "prevenção e repressão dos crimes". Para COSTA ANDRADE serão inadmissíveis as ações exclusivamente repressivas por constituírem um meio enganoso de prova reconduzível aos métodos proibidos de prova nos termos da alínea a) do n.º2 do art. 126.º do CPP. Admite apenas as ações exclusivamente preventivas em casos de "desmantelamento de *terrorismo, criminalidade violenta ou altamente organizada*" (itálicos no original).

[8] MANUEL AUGUSTO ALVES MEIREIS, *O Regime das Provas Obtidas pelo Agente Provocador Em Processo Penal*, 1999, p. 192
[9] ISABEL ONETO, *O agente infiltrado- Contributo para a compreensão do regime jurídico das ações encobertas*, 2005, p. 139

Conclui o autor que, caso assim não fosse, "deixar-se-ia a sociedade desarmada face a manifestações tão drásticas e intoleráveis de criminalidade".[10]

No que concerne, em específico, aos tipos de ações encobertas estas podem ser: *light cover* e *deep cover*. Esta denominação tem por base a atuação e o nível de infiltração do agente. As primeiras caraterizam-se por durarem menos de seis meses, não têm um plano minucioso e o agente pode manter a sua identidade dado o risco destas ações ser menor. Já as segundas, são ações de longa duração em que o agente adota uma identidade fictícia (art. 5.º do RJAE) para a sua segurança dados os riscos que corre com a sua inserção no meio criminoso[11].

The last, but not least, temos que fazer nota à possibilidade de estas ações serem realizadas com recurso a terceiros sob direção da PJ. As razões podem ser várias podendo desde já ser avançadas duas: esse terceiro já se encontra integrado no meio criminoso ou pode ter acesso a informações e ter conhecimentos específicos de extrema utilidade para a investigação.[12]

2.2. Artigo 2.º "Âmbito de aplicação"

O recurso às AE deve ser realizado com especial "parcimónia e o modo como se desenvolvem deve ser objeto de aprofundado escrutínio"[13]. Como tal, é previsto neste artigo um catálogo taxativo de crimes que admitem recurso a estas ações[14].

A grande inovação do RJAE é o alargamento do catálogo de crimes. Como vimos, a primeira abordagem a esta figura centrava-se em crimes de tráfico de estupefacientes e de substâncias psicotrópicas sendo, mais tarde, alargado o seu âmbito aos crimes de corrupção

[10] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova*…, ob. cit., pp. 231-233
[11] ISABEL ONETO, *O agente infiltrado…,* ob.cit., pp. 81- 84
[12] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 298
[13] Ac. do TRL de 23 de março de 2011, Processo n.º 182/09.6JELSB.L1-5 disponível em www.dgsi.pt
[14] Para além deste catálogo temos um alargamento a outros crimes em que se admite o recurso a Ações encobertas nos artigos 19º da Lei n.º 109/2009 de 15 de setembro (Lei do Cibercrime), no art. 160º-B da Lei n.º 144/99 de 31 de agosto (Lei da Cooperação Judiciária Internacional em matéria penal) e no art. 188º da Lei n.º 23/2007 de 4 de julho (Regime Jurídico de entrada, permanência, saída e afastamento de estrangeiros do território nacional)

e de criminalidade económico financeira. Dada a necessidade de combater a "globalização da criminalidade transnacional"[15] tem que se "responder com a globalização da repressão da criminalidade"[16]. Assim, passou-se a admitir-se o uso a AE em crimes como: a) homicídio voluntário; b) os crimes contra a liberdade e contra a autodeterminação sexual a que corresponda, em abstrato, pena superior a 5 anos de prisão, desde que o agente não seja conhecido, ou sempre que sejam expressamente referidos ofendidos menores de 16 anos ou outros incapazes; c) Relativos ao tráfico e viciação de veículos furtados ou roubados; d) Escravidão, sequestro e rapto ou tomada de reféns; e) Tráfico de pessoas[17]; f) Organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo[18]; g) Captura ou atentado à segurança de transporte por ar, água, caminho-de-ferro ou rodovia a que corresponda, em abstrato, pena igual ou superior a 8 anos de prisão; h) Executados com bombas, granadas, matérias ou engenhos explosivos, armas de fogo e objetos armadilhados, armas nucleares, químicas ou radioativas; i) Roubo em instituições de crédito, repartições da Fazenda Pública e correios; j) Associações criminosas; l) Relativos ao tráfico de estupefacientes e de substâncias psicotrópicas; m) Branqueamento de capitais, outros bens ou produtos; n) Corrupção, peculato e participação económica em negócio e tráfico de influências; o) Fraude na obtenção ou desvio de subsídio ou subvenção; p) Infrações económico-financeiras cometidas de forma organizada ou com recurso à tecnologia informática; q) Infrações económico-financeiras de dimensão internacional ou transnacional; r) Contrafação de moeda, títulos de créditos, valores selados, selos e outros valores equiparados ou a respetiva passagem; s) Relativos ao mercado de valores mobiliários.

Podemos constatar que o catálogo atual se afigura extenso e "bem mais permissivo"[19], sendo possível o recurso às AE em crimes contra as pessoas, contra o património, contra a vida em sociedade e contra o Estado. Acompanhamos a visão de SANDRA PEREIRA quando esta refere que este elenco extenso "dá um sinal preocupante:

---

[15] Discurso do Ministro da Justiça António Costa na Reunião plenária de 21 de junho de 2001, publicada no Diário da Assembleia da República de 22 de junho de 2001, I Série- Número 99, p. 16. Disponível em: https://debates.parlamento.pt/catalogo/r3/dar/01/08/02/099/2001-06-21/16, acedido a 27-01-2021

[16] *Ibid.*

[17] Alínea aditada pela Lei n.º 60/2013 de 23 de agosto

[18] No que diz respeito ao terrorismo internacional e financiamento do terrorismo estes foram aditados pela Lei n.º 61/2015 de 24 de junho

[19] SANDRA PEREIRA, "A recolha de prova pelo agente infiltrado" *in Prova Criminal e direito de defesa: estudos sobre a teoria da prova e garantias de defesa em processo penal*, 2017, p. 149

o de tornar este método como algo banal e generalizado"[20]. Dado o caráter excecional deste método e potencial lesão de DF's o alargamento feito pelo legislador é questionável. Este método deverá ser utilizado para "proteger "bens jurídicos de transcendente importância" do individuo ou da comunidade"[21] e apenas quando todos os outros métodos tradicionais se afigurem inúteis.

2.3. Artigo 3.º "Requisitos" e Artigo 4.º "Proteção de funcionário e terceiro"

Quanto aos requisitos, consagrou o legislador, no n.º 1 do art. 3.º, que o recurso a estas ações só será admissível quando estas se revelem adequadas e proporcionais às finalidades de prevenção e repressão e, também, à gravidade do crime. Estamos perante a consagração do princípio da proporcionalidade, ou da proibição do excesso, previsto no n.º 2 do art. 18.º da CRP[22], que tem como corolários a adequação, a necessidade e a proporcionalidade *stricto sensu*. Assim, a AE terá que se revelar adequada à prossecução dos fins visados; terá que ser necessária, revelando-se como o único meio eficaz e útil para a prossecução daqueles mesmos objetivos; e, por fim, terá que obedecer à proporcionalidade *stricto sensu* fazendo-se uma ponderação global entre a gravidade da intromissão e as razões que a justificam[23], ou seja, deverá ser ponderado, em concreto, se o recurso a uma AE (sabendo do seu caráter potencialmente lesivo) se afigura excessivo tendo em conta a gravidade do crime e o fim visado. Relacionado com este princípio da proporcionalidade, em específico com o corolário da necessidade, temos o princípio da subsidiariedade na aplicação dos métodos ocultos de investigação criminal.[24] Refere COSTA ANDRADE que terá que se ter em atenção, no plano extrínseco, a todos os meios abertos que se tem ao dispor. Caso se revele que estes não são suficientes para satisfazer o fim pretendido há que, no plano intrínseco, atender à relação dos meios entre si e escolher o menos gravoso que, ao mesmo tempo, seja idóneo (como o ilustre autor exemplifica, se for possível recorrer a uma

[20] *Ibid.*
[21] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado*"*, ob. cit., p. 124
[22] Este artigo diz-nos que "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos."
[23] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob. cit., p. 116
[24] *Ibid*. p. 115

escuta telefónica não se deverá proceder à gravação de uma conversa entre presentes)[25]. Se existir cumulação de métodos ocultos, tal só será admitido caso a utilização de apenas um não realize o resultado probatório. Esta possibilidade reserva-se para casos extremos e de elevada danosidade ou sofisticação criminal.

No n.º 2 estabelece-se que "Ninguém pode ser obrigado a participar em ação encoberta". Tal resulta da consciência que a segurança dos agentes participantes de uma AE pode ser comprometida dada sua a inserção no meio criminoso e, também, pelo perigo de eventuais represálias.[26] Esta preocupação com a segurança do AE está, também, presente no art. 4.º salientando-se o disposto no n.º3 que prevê a possibilidade de o agente que tenha atuado ao abrigo de identidade fictícia possa, oficiosamente ou a requerimento, prestar depoimento sob essa mesma identidade.

Dado que esta figura contende com DF's estabeleceu-se a necessidade de prévia autorização para a realização da AE por autoridade judiciária- MP ou JIC- conforme estabelece o n.º3 e n.º4 deste art. 3.º: "3 - A realização de uma ação encoberta no âmbito do inquérito depende de prévia autorização do competente magistrado do Ministério Público, sendo obrigatoriamente comunicada ao juiz de instrução e considerando-se a mesma validada se não for proferido despacho de recusa nas setenta e duas horas seguintes. 4 - Se a ação referida no número anterior decorrer no âmbito da prevenção criminal, é competente para autorização o juiz de instrução criminal, mediante proposta do Ministério Público."

No domínio da prevenção criminal, para que a AE se realize terá que ser o JIC a autorizar, mediante proposta do MP. No âmbito do inquérito, o MP será quem emite despacho a autorizar a AE sendo depois comunicado ao JIC. Assim, esta autorização está sujeita a deferimento tácito (considera-se validada se não for proferido despacho judicial de recusa nas 72h seguintes) ou expresso por parte do JIC (art. 3.º, n.º 3 e 4 do RJAE).

Dado o exposto no n.º 4 do art. 32.º e no n.º2 do art. 202.º da CRP, será ao JIC, enquanto juiz das liberdades,[27] que cabe analisar objetivamente quais os bens jurídicos que

---

[25] *Ibid*. pp. 114-115

[26] Discurso do Ministro da Justiça António Costa na Reunião plenária de 21 de junho de 2001, publicada no Diário da Assembleia da República de 22 de junho de 2001, I Série- Nº 99, p. 16. Disponível em: https://debates.parlamento.pt/catalogo/r3/dar/01/08/02/099/2001-06-21/16, acedido a 27-01-2021

[27] MARIA JOÃO ANTUNES, *Direito Processual Penal*, 2017, p. 81

se encontram em conflito e, perante a proposta do MP, decidir se a restrição dos DF's, naquele caso em concreto e dados os fins prosseguidos, se justifica. É de extrema importância este papel do juiz dado não haver lugar ao contraditório por parte do titular do direito lesado. Assim, perante a proposta do MP, o juiz deverá autorizar (total ou parcialmente) a AE ou, pelo contrário, indeferir. Quando autorize a ação, deve fundamentar referindo quais as razões que o levaram àquela decisão, a delimitação temporal, os moldes da AE, pessoas visadas, meios a utilizar,… Tal como, caso indefira, tem que elencar as razões de facto e de direito que o levam àquela decisão. Será de extrema importância a fundamentação no caso de autorização da AE porque será nesta que o arguido encontrará a justificação do recurso a esta ação[28]. Apesar de referirmos a necessidade de fundamentação por parte do JIC, a verdade é que a prática revela-se outra. Existe uma tendência para a adesão acrítica ao pedido formulado pelo MP, frustrando totalmente o papel do JIC enquanto garante dos interesses da pessoa visada pela medida[29].

No final desta AE, a PJ fará o relato da intervenção do AE à autoridade judiciária competente no prazo máximo de 48 horas após o termo daquela (n.º6 art. 3.º RJAE). A junção deste relato ao processo só se verifica em casos de extrema indispensabilidade probatória (n.º1 do art. 4.º). A apreciação desta indispensabilidade pode ser remetida, nos termos do n.º2, para o termo da fase de inquérito ou instrução. Se o juiz entender pela indispensabilidade da prova e determinar a comparência do AE em audiência de julgamento terá sempre que ser observado o disposto no n.º1 do art. 87.º do CPP e da Lei n.º 93/99 de 14 de julho (Lei de Proteção das Testemunhas).

2.4. Artigo 5.º "Identidade fictícia"

É prevista a possibilidade de o agente atuar ao abrigo de identidade fictícia. Porém, como estabelece o n.º1 do art. 5.º, apenas aos agentes de polícia criminal lhes é concedida esta possibilidade. Esta identidade é válida por seis meses prorrogáveis e é atribuída por despacho do Ministro da Justiça. Nesta possibilidade de atuação ao abrigo de identidade

[28] DAVID SILVA RAMALHO, *Métodos Ocultos…,* ob. cit., p. 238; MANUEL DA COSTA ANDRADE, "Métodos ocultos... *",* ob. cit., p. 549
[29] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob. cit., p. 119

fictícia temos presente, mais uma vez, a preocupação com a segurança destes agentes. Iremos abordar esta questão de forma mais detalhada *infra* no domínio virtual.

2.5 Artigo 6.º "Isenção de Responsabilidade"

Durante a sua atuação, o AE poderá praticar alguns atos que preencham um tipo legal ilícito. Assim, no n.º1 do art. 6.º, temos uma cláusula de isenção da responsabilidade estabelecendo-se que, durante a AE, o agente pode praticar atos preparatórios (não puníveis pelo art. 21.º do CP) e de execução (n.º2 do art. 22.º do CP) desde que tal não consubstancie autoria mediata ou instigação. Assim, toda a atuação do AE se encontra limitada por esta cláusula devendo este atuar com o máximo respeito pelo previsto na norma. Este artigo assume particular importância na diferenciação entre a infiltração e a provocação que iremos explorar de seguida.

3. Os "homens de confiança"

Como já sabemos, o AE é encarado como um método oculto de obtenção de prova. Cabe agora estudar os atores envolvidos nessa ocultação. Já vimos que estamos perante um agente que atua "com ocultação da sua qualidade e identidade" (n.º2 do art.1º do RJAE). Contudo, este agente poderá ser encarado como encoberto/infiltrado ou um provocador. Será à delimitação conceptual e elaboração de fronteiras entre o que é infiltração e o que é provocação que iremos dedicar as próximas linhas.

Tomamos como ponto de partida a noção (extensa) de homens de confiança avançada por COSTA ANDRADE que abrange "todas as testemunhas que colaboram com as instâncias formais da perseguição penal […]. Cabem aqui tanto os particulares […] como os agentes das instâncias formais […]; e quer se limitem à escolha de informações […], quer vão ao ponto de provocar eles próprios a prática do crime".[30]

[30] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova*…, ob. cit., p. 220

Considerando que a base deste conceito de homens de confiança é o acesso a informação privilegiada por quem pertence ao meio criminoso, hoje podemos enunciar mais duas figuras fundamentais na investigação criminal: o *whistleblower* e o colaborador premiado. O primeiro é "alguém que, fazendo parte da organização […] denuncia, […] a prática daqueles ilícitos"[31] ou seja, "sinaliza um comportamento ilegal"[32]. Já o segundo, será aquele que faz parte da organização criminosa só que, ao ser investigado criminalmente, decide colaborar com as autoridades beneficiando em termos punitivos[33]. Em ambos, as autoridades acabam por ter "acesso a informação reservada"[34].

Veremos *infra*[35] a propósito da infiltração *online* e da adoção de identidade fictícia que a figura do homem de confiança se pode revelar bastante útil pois pode permitir, pelos conhecimentos específicos que este possui do meio criminoso e, ocasionalmente, pelos seus conhecimentos técnicos, o acesso pelas autoridades às informações necessárias para que a investigação prossiga.

3.1. O agente provocador numa perspetiva doutrinal

Como vimos acima, a figura do AE cria algumas controvérsias na doutrina especialmente na distinção desta do agente infiltrado. O que, como referimos anteriormente, não consideramos ser profícuo. O agente provocador, por sua vez, é uma figura mais pacífica na doutrina. A maioria, conduz esta figura à sua inadmissibilidade. Assim, iremos fazer uma análise sobre o que nos ensina a doutrina a propósito deste agente e em que medida se afigura possível desenhar uma fronteira entre a provocação e a infiltração.

Para GERMANO MARQUES DA SILVA, o agente infiltrado carateriza-se por não participar na prática do crime isto porque "a sua atividade não é constitutiva, mas apenas

[31] SUSANA AIRES DE SOUSA, *Ações Encobertas (e outras figuras próximas) na investigação da criminalidade económico-financeira*, *in* revista JULGAR, n. º38, 2019, p. 40
[32] NUNO BRANDÃO, *O whistleblowing no ordenamento jurídico português,* RMP 161: janeiro: março 2020, p. 99
[33] SUSANA AIRES DE SOUSA, *Ações Encobertas…* ob.cit., p. 40
[34] *Ibid.*
[35] Cap. II, ponto 3.3

informativa"[36]. Já o agente provocador será aquele que "cria o próprio crime e o próprio criminoso"[37]. Este último afigura-se absolutamente "inaceitável […] como método de investigação criminal, uma vez que gera o seu próprio objeto".[38]

ISABEL ONETO defende que o agente infiltrado tem uma conduta ativa, é um participante ativo[39] da atividade criminosa, convivendo com os criminosos, ganhando a sua confiança apenas estando vedada a sua atuação como instigador e como autor mediato segundo o disposto no n.º1 do art. 6.º do RJAE[40]. Será neste ponto que encontramos a fronteira entre a infiltração e a provocação. O agente infiltrado beneficia, pelo artigo referido, de um regime que exclui a sua responsabilidade penal se este atuar nos trâmites previstos, enquanto o agente provocador está sujeito às regras gerais. O AE não provoca o crime, o agente provocador instiga e cria em outrem a decisão criminosa. [41]

Para SANDRA PEREIRA o agente infiltrado será "aquele sujeito (agente da autoridade ou terceiro por si comandado) que não determina outrem à prática do crime, mantendo-se à margem da formação da vontade de cometer o ilícito criminal"[42]. O agente provocador, por sua vez, aparecerá como um instigador sendo o ator principal no acontecimento criminoso.

Já ANTÓNIO HENRIQUES GASPAR define o agente provocador como o "agente da autoridade policial ou um terceiro por esta controlado que dolosamente determina outrem à comissão de um crime, o qual não seria cometido sem a sua intervenção, movido pelo

[36] GERMANO MARQUES DA SILVA, *Bufos, Infiltrados, Provocadores e arrependidos, Os princípios democrático e da lealdade em processo penal* in Direito e Justiça, 1994, página 31
[37] GERMANO MARQUES DA SILVA, *Meios processuais expeditos no combate ao crime organizado (A Democracia em perigo?)* in Lusíada.Direito, n.º3, 2005, p. 76
[38] *Ibid.*,
[39] ISABEL ONETO, *O agente infiltrado*…, ob. cit., pp. 137-138
[40] Neste artigo dispõe-se que "Não é punível a conduta do agente encoberto que, no âmbito de uma ação encoberta, consubstancie a prática de atos preparatórios ou de execução de uma infração em qualquer forma de comparticipação diversa da instigação e da autoria mediata, sempre que guarde a devida proporcionalidade com a finalidade da mesma."
[41] ISABEL ONETO, *O agente Infiltrado*…, ob. cit., p. 145
[42] SANDRA PEREIRA, "A recolha de prova por agente infiltrado", ob. cit., p. 143

desejo de obter provas da prática desse crime ou de submeter o autor do facto a um processo penal e à condenação"[43]

Concluímos que, em termos teóricos, e pelo que o RJAE nos ensina, o que separa a infiltração da provocação prende-se com atuação do agente comportar instigação ou autoria mediata[44] (n.º1 do art. 6.º do RJAE). Traçamos o agente provocador como alguém que convence outrem à prática de um crime, determinando a sua vontade e criando neste a decisão criminosa que, antes da intervenção do agente provocador, não existia. Será ele próprio que cria o crime. Tal representa um desrespeito pelos DF's, caindo fora do âmbito do art. 6.º do RJAE e, por isso mesmo, inadmissível no OJ português. À prova obtida através da provocação será aplicado o regime constante dos arts. 125.º e da alínea a) do n.2 do art. 126.º do CPP conjugados com o n.º8 do art. 32.º da CRP sendo toda a prova obtida declarada nula em virtude de estarmos perante um "método proibido de prova". Assim, não são admitidas provas que pressuponham uma afronta à dignidade humana, à liberdade de decisão ou vontade e à integridade física ou moral das pessoas.[45] Se se revela aparentemente fácil a delimitação a um nível teórico, no que diz respeito à prática e às decisões dos tribunais deparamo-nos com algumas dificuldades sentidas pelos magistrados em reconduzir a atuação do agente à infiltração ou à provocação. Como vimos, ao AE é permitida a prática de factos típicos (desde que tal não consubstancie instigação ou autoria mediata), mas quando é que essa atuação se traduz em provocação? Iremos analisar o que tem entendido a jurisprudência a nível internacional com o caso Teixeira de Castro vs. Portugal e a nível nacional com um percurso pela jurisprudência do TC, STJ e TRL.

[43] ANTÓNIO HENRIQUES GASPAR, "As ações encobertas e o processo penal: questões sobre a prova e o processo equitativo" in *Medidas de Combate à Criminalidade Organizada e Económico-Financeira,* 2004, p.46.

[44] A Autoria Mediata encontra-se prevista no art. 26º do CP sendo a 2º modalidade de autoria aí prevista "(quem executar (…) por intermédio de outrem") e traduz-se, segundo a teoria do domínio do facto, na circunstância de todo o acontecimento criminoso ser obra do "homem-de-trás". No que concerne à Instigação (4º modalidade de autoria) esta encontra-se prevista no mesmo artigo no segmento "ainda quem, dolosamente, determinar outra pessoa à prática do facto", ou seja, será instigador aquele que determinar outrem à prática de um facto típico ilícito. Cf.: JORGE DE FIGUEIREDO DIAS, *Direito Penal- Parte Geral*, 2019, pp. 905-906 e 930-931

[45] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova …,* ob.cit., 2013, p.216

3.2. A linha ténue[46] que separa a infiltração da provocação- dificuldades práticas

No que diz respeito à jurisprudência firmada a propósito do tema ainda são visíveis dificuldades de distinção prática das figuras do AE e do agente provocador.

Não podemos deixar de começar por um dos casos mais importantes para o estudo do tema: Teixeira Castro contra Portugal. A importância deste caso reside no facto de, pela primeira vez, um Estado ter sido condenado por ter feito uso de um agente provocador[47]. O caso prendia-se com uma investigação de tráfico de droga com a intervenção de dois agentes da PSP que se faziam passar por compradores de droga com o propósito de chegar a uma pessoa específica: o fornecedor Teixeira de Castro.[48] Na verdade, estes agentes conseguiram arquitetar um encontro, através de um outro suspeito com quem mantinham contacto, com Teixeira de Castro para que este lhes fornecesse heroína[49]. Quando o encontro se consumou os dois agentes da PSP acabaram por proceder à detenção de Teixeira de Castro que tinha na sua posse, além da heroína a ser fornecida aos agentes da PSP, "outras duas saquetas de heroína, uma soma de 43.000 escudos e uma pulseira de ouro"[50]. Já no âmbito do processo criminal desencadeado após a sua detenção, Teixeira de Castro viu o Tribunal de Primeira instância condená-lo a 6 anos de pena de prisão. Não satisfeito com a decisão, apresentando como tese que os agentes teriam atuado como provocadores, apresentou recurso. Perante o não provimento pelo STJ[51], este recorreu para o TEDH. Este tribunal teve uma visão diferente que os outros haviam tido e acabou por condenar o Estado Português por violação do art. 6.º da CEDH ("Direito a um Processo Equitativo")[52]. Sustentou a sua decisão afirmando que os agentes provocaram a atividade criminosa e que, sem a sua intervenção, não haveria lugar àquele crime o que afetava de forma irremediável o caráter justo do

[46] Ac. do TC n.º 578/98 de 14 de outubro de 1998 disponível em www.tribunalconstitucional.pt/tc/acordaos
[47] CAROLINA PEREIRA, *O Entendimento Jurisprudencial do Tribunal Europeu dos Direitos do Homem (TEDH) acerca da atuação do Agente Infiltrado* in RIDB, Ano 1 (2012), nº 11, p. 6948;
[48] *Ibid*., p. 6949
[49] SUSANA AIRES DE SOUSA, *Agent Provocateur e meios enganosos de prova. Algumas reflexões*, in Liber Discipulorum para Jorge de Figueiredo Dias, 2003, p. 1232
[50] CAROLINA PEREIRA, *O Entendimento Jurisprudencial…* ob cit., p. 6950
[51] SUSANA AIRES DE SOUSA, *Agent Provocateur …* ob.cit., p. 1233
[52] ISABEL ONETO, *O agente Infiltrado*… ob. cit., p. 134

processo[53]. Porém, outro juiz (Butkevych)[54], votando inclusive contra, teria uma outra visão afirmando que os agentes teriam atuado como infiltrados dado que a intenção criminosa em Teixeira de Castro já existia tendo este consciência da ilicitude da sua conduta e saber ou não a identidade dos polícias em nada iria alterar a substância do caso. Acrescenta que a restrição aos DLG's seria admissível tendo que se tentar encontrar um equilíbrio entre essa restrição e os perigos que se pretendem acautelar.

A nível nacional, comecemos por fazer referência ao Acórdão do TC n.º 578/98 de 14 de outubro de 1998. Temos assente que "é inquestionável a inadmissibilidade da prova obtida por agente provocador, pois seria imoral que, num Estado de Direito, se fosse punir aquele que um agente estadual induziu ou instigou a delinquir. Uma tal desonestidade seria de todo incompatível com o que, num Estado de Direito, se espera que seja o comportamento das autoridades e agentes da justiça penal, que deve pautar-se pelas regras gerais da ética". Quanto ao AE o tribunal afirma ser "impossível renunciar ao serviço do *undercover agent*" dados "os meios, de que os criminosos dispõem, tantos e tão sofisticados, que a sociedade quase se sente impotente para dar combate a tal criminalidade. E, por isso, aceita-se aqui alguma excecionalidade no modo de obter as prova". Portanto, para meios excecionais, métodos excecionais.

No que toca à jurisprudência do STJ, este tem vindo a entender que a atuação do "agente provocador é normalmente considerada como ilegítima"[55]. Assim, na prática, importa fazer distinção das situações em que a realização de uma intenção criminosa é criada que era até então inexistente, daquelas em que o sujeito já está potencialmente inclinado a delinquir e a atuação do agente apenas faz com essa se coloque em prática. Tem-se vindo a entender, também, que o agente provocador representa um ato de deslealdade afetando a cultura jurídica democrática e a legitimação do processo penal que a acolhe.[56] Assim, esta figura é reconduzida a um meio enganoso de prova previsto na alínea a), n.º2 do art. 126.º

---

[53] "*In the light of all these considerations, the Court concludes that the two police officers' actions went beyond those of undercover agents because they instigated the offence and there is nothing to suggest that without their intervention it would have been committed. That intervention and its use in the impugned criminal proceedings meant that, right from the outset, the applicant was definitively deprived of a fair trial. Consequently, there has been a violation of Article 6 § 1."* Ac. Teixeira de Castro vs Portugal de 9 de junho de 1998 disponível em: TEIXEIRA DE CASTRO v. PORTUGAL (coe.int)

[54] CAROLINA PEREIRA, *O Entendimento Jurisprudencial…* ob cit., p. 6956.

[55] Ac. STJ de 20 de fevereiro de 2003, processo n.º 02P4510, disponível em www.dgsi.pt

[56] Ac. STJ de 13 de janeiro de 1999, processo n.º 999/98, disponível em www.dgsi.pt

do CPP. Entende-se ser agente provocador aquele que cria uma intenção criminosa num suspeito, que era, até àquele momento, inexistente. Sem a intervenção deste agente, o facto ilícito não teria lugar[57]. Por sua vez, o infiltrado/encoberto insinua-se junto dos agentes do crime, ocultando a sua identidade e qualidade, de modo a ganhar a sua confiança para obter informações, sem nunca os determinar à prática de infrações.

Para melhor percebermos o cerne da questão analisemos comparativamente decisões do STJ de 20 de fevereiro de 2003 (Processo n.º: 02P4510) e do TRL de 20 de maio de 2010 (Processo n.º: 281/08.1JELSB.L1-5)[58]. O objetivo será perceber as dificuldades sentidas na prática.

Em ambos os casos estamos na presença de crimes de tráfico de estupefacientes e colaboração de um terceiro com a PJ. No caso do STJ, temos a atuação de "S" que havia sido contactado para se inserir numa operação de tráfico de estupefacientes. Após isto, ofereceu-se para colaborar com a PJ e lhes dar informações importantíssimas da operação a troco de determinada quantia monetária. Já no segundo caso, no do TRL, temos um terceiro "M" que colabora com a PJ e que, na altura dos factos, se encontrava detido (sendo posteriormente condenado) pelo crime de tráfico de 120kg de cocaína. Este tomou conhecimento de que "J" estava a planear uma operação de tráfico de estupefacientes e, fazendo uso disso, informou a PJ que estaria disposto a fornecer algumas informações em troca de uma atenuação da sua pena.

No que toca às perspetivas dos tribunais, o STJ que entendeu que a atuação de "S" se enquadrava no âmbito do RJAE e, por isso, era legítima. Afirmou o tribunal que "o(s) agente(s) infiltrado(s) não induziram ninguém a praticar um crime de importação de cocaína por Portugal com envio para Espanha e distribuição pela Europa, pois esse projeto já estava em marcha quando aquele que viria a ser agente infiltrado foi contactado, como nunca deixaram de ter os seus autores do domínio do facto".

Já o TRL, entendeu que a atuação de "M" constituía uma verdadeira provocação entendendo que este "convenceu dolosamente o arguido J… à prática de um crime, fazendo-

[57] Ac. TRL de 22 de março de 2011, processo n.º 182/09.6JELSB.L1-5, disponível em www.dgsi.pt
[58] Ambos os Acórdãos disponíveis em www.dgsi.pt

lhe crer que teria os contactos necessários". Por conseguinte, toda a prova obtida foi declarada nula e "J" absolvido.

Estamos perante, como constatamos, situações faticamente semelhantes, mas com decisões e enquadramentos distintos. Fica clara a dificuldade que a jurisprudência tem em qualificar uma conduta de infiltração ou de provocação.

CAPÍTULO II. O Agente Encoberto Digital

1. Cibercriminalidade: um novo desafio para o Processo Penal

Desde o início do presente século, temos assistido a uma verdadeira "revolução tecnológica"[59] que se manifesta nos mais variados campos da sociedade desde a cultura, economia, saúde e, claro, a justiça. Se, por um lado, a Internet se tornou numa das melhores invenções de sempre, no que à criminalidade diz respeito somos confrontados com novos instrumentos e formas de criminalidade. Assistimos a uma "*deslocação criminosa para a Web*"[60] (itálico no original), existindo a tendência para as pessoas praticarem crimes online que, muito provavelmente, não praticariam por outros meios. E uma "*deslocação criminosa na Web*"[61] traduzindo-se na facilidade de fuga à aplicação da lei através da transferência de informações de um ponto que haja sido encerrado pelas autoridades para um outro ponto na Web, eventualmente noutro país.

Este fenómeno está a ascender de forma galopante. No ano transato, marcado pela pandemia de COVID-19, assistimos a um aumento da cibercriminalidade. De acordo com o Relatório Anual de Segurança Interna de 2020[62] "o ano foi inevitavelmente marcado, ao nível da cibersegurança, pela pandemia de COVID-19. Notou-se um considerável aumento do número de incidentes, principalmente a partir do mês de março, coincidindo com o primeiro estado de emergência declarado a 13 de março. Os números podem ser justificados por um conjunto de fatores, tais como, o incremento do tempo de utilização do ambiente digital, incluindo o social, o incremento do teletrabalho e a consequente diluição da tradicional segurança perimétrica das organizações ou o incremento do recurso ao comércio eletrónico".

Estabelecemos como ponto de partida o que aprendemos com FIGUEIREDO DIAS que nos diz "as soluções concretas dos problemas básicos do Direito Processual Penal dependam fundamentalmente do estádio de evolução e desenvolvimento social e cultural de

[59] Expressão utilizada por FEDERICO BUENO DE MATA, *El Agente Encubierto en Internet: Mentiras Virtuales para alcanzar la Justicia*, 2012, p. 1
[60] PEDRO DIAS VENÂNCIO, *Lei do Cibercrime* Anotada e Comentada, 2011, p. 15
[61] *Ibid.*
[62] Disponível em: ficheiro.aspx (portugal.gov.pt), p. 160, consultado em 31/3/2021

uma certa comunidade"[63]. Assim, o processo penal que hoje conhecemos não é o mesmo de há algumas décadas atrás. As sociedades mudam, os meios para cometimento de crimes mudam e, como tal, tem que existir uma adaptação legislativa às mutações registadas.

Para tanto, surgem algumas respostas a nível europeu. O principal diploma a analisar, inicialmente, no nosso estudo será a Convenção do Cibercrime. Porém, antes desta foram adotadas algumas recomendações elaboradas pelo Comité de Ministros do Conselho da Europa como a Recomendação N.º (89) 9 e a R (95) 13. Tendo como matriz a R (89)9, Portugal legislou em matéria de criminalidade informática através da Lei nº 109/91 de 17 de agosto. Esta veio a ser revogada pela Lei nº 109/2009 de 15 de setembro que é a atual LC resultado da transposição para o nosso ordenamento jurídico da Decisão-Quadro n.º 2005/222/JAI do Conselho da Europa.[64]

2. A Convenção sobre o Cibercrime

A CCiber do Conselho da Europa de 23 de novembro de 2001 foi o primeiro diploma internacional que versou sobre a cibercriminalidade. O que se pretendeu com o tratado foi a harmonização das várias legislações no tema da criminalidade sobre computadores, redes e dados oferecendo-se mecanismos aos países que facilitem a cooperação internacional e a própria investigação criminal[65].

Do Relatório Explicativo[66] da Convenção resultam, no parágrafo 16, os objetivos principais do diploma que assentam no seguinte: 1) a harmonização das legislações dos Estados signatários no tema da cibercriminalidade; 2) criar no âmbito da legislação processual medidas que permitam às autoridades a recolha de prova; e 3) estabelecer mecanismos que propiciem um regime mais eficaz e rápido no que concerne à cooperação internacional.

---

[63] JORGE DE FIGUEIREDO DIAS, *Direito Processual Penal*, reimpressão da 1.ª Edição de 1974, 2004, p. 59.

[64] Esta veio a ser substituída, mais tarde, pela Diretiva 2013/40/UE DO PARLAMENTO EUROPEU E DO CONSELHO de 12 de agosto de 2013 relativa a ataques contra os sistemas de informação

[65] PEDRO VERDELHO, ROGÉRIO BRAVO, MANUEL LOPES ROCHA, *Leis do Cibercrime*- Vol. I., p. 10

[66] Disponível em: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf consultado em 31/3/2021

Para dar cumprimento a estes objetivos, o diploma é dividido em quatro capítulos[67]. De uma forma geral, a CCiber incide sobre direito penal material (definindo crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes cometidos por via da informática), mas inclui também medidas processuais e de cooperação judiciária internacional[68].

A) Direito Penal Material

O primeiro artigo diz respeito à terminologia, definindo alguns dos conceitos relevantes. Algumas das definições previstas na CCiber já se encontravam previstas na LCI, porém este diploma internacional estabelece novidades como os conceitos de "dados informáticos", "dados de tráfego" e "prestador de serviços".[69]

O segundo capítulo, fixado entre os arts. 2.º a 22.º, diz respeito às medidas a adotar a nível nacional. Na sua primeira secção (art. 2.º a 13.º), estabelecem-se os tipos de infrações sendo estas divididas em títulos.

Na sua maioria, estes já se encontravam previstos no OJ português, mais concretamente, na LCI. Surgem, contudo, alguns novos tipos legais e outros que poderão ser ajustados.

Assim, temos, entre os arts. 2.º e 10.º, alguns crimes como: o Acesso Ilícito, Interceção Ilícita, Dano provocado nos dados, Sabotagem informática e Utilização Indevida de Dispositivos, Falsificação Informática, Burla Informática, Infrações relativas à Pornografia Infantil e Infrações relativas à Violação de Direitos de Autor e dos Direitos Conexos. Entre os arts. 11.º a 13.º, temos outras formas de responsabilidade e sanções. A verdadeira novidade que a CCiber institui neste âmbito é o disposto no art. 6.º que diz respeito à utilização indevida de dispositivos. Apesar disso, segundo o nº3 deste mesmo artigo, abre-se a hipótese para "cada parte (…) reservar-se o direito de não aplicar o n. º 1 do presente artigo, desde que essa reserva não diga respeito à venda, distribuição ou qualquer outra forma de disponibilização". Outra questão nova aquando da elaboração da CCiber prende-se com o disposto na alínea e) do n.º1 art. 9.º que prevê a ilicitude da posse de

[67] Diploma disponível em: https://www.cicdr.pt/documents/57891/128776/Convenção+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c consultado em 21/03/2021
[68] Exposição de motivos PROPOSTA DE LEI N.º 289/X/4ª, p. 2
[69] PEDRO VERDELHO, ROGÉRIO BRAVO, MANUEL LOPES ROCHA, *Leis do Cibercrime*…, ob. cit., p. 11.

pornografia infantil em sistema informático. Tal, à época, não se encontrava previsto no CP. A Lei nº 99/2001 de 25 de agosto agiu nesta linha, porém de uma forma mais restrita ao estabelecer a punição, na alínea e) do art. 172.º do CP, de quem "e) Detiver materiais previstos na alínea c), com o propósito de os exibir ou ceder". Ou seja, a posse de pornografia infantil apenas seria punível caso o propósito fosse a exibição ou cedência da mesma. Atualmente, na alínea d) do n.º 1 do art. 176.º manteve-se esta possibilidade de punir a conduta de quem detenha pornografia infantil com o propósito de "distribuir, importar, exportar, divulgar, exibir ou ceder" constituindo um crime de intenção.[70] Porém, no n.º 5 do art. 176.º do CP temos prevista a possibilidade de punição da posse de pornografia infantil, mas sem a exigência do propósito, por parte do agente, de exibir ou ceder tais conteúdos ("*detenção pura*[71]").

Todos os outros crimes enunciados já se encontravam previstos na lei portuguesa com um conteúdo semelhante ao disposto na CCiber.

B) Direito Processual

Na segunda secção do mesmo capítulo temos as questões processuais (art. 14.º a 21.º). Estabelece-se, logo no art. 14.º, que cada uma das partes signatárias deve "adotar as medidas legislativas e outras que se revelem necessárias para instituir os poderes e os procedimentos previstos na presente secção, para efeitos de investigação ou de procedimento criminal específicos".

Para tal, a CCiber adota algumas medidas clássicas como as buscas e apreensões (art. 19.º) introduzindo uma novidade: a conservação expedita de dados (arts. 16.º e 17.º). Estas últimas são de extrema importância para a investigação criminal pois permitem a preservação de dados com considerável rapidez, essencial na investigação. O mecanismo previsto no art. 18.º também constitui uma novidade. Possibilita que as autoridades competentes ordenem, às pessoas singulares ou coletivas, o fornecimento de dados

[70] Os crimes de intenção ou de resultado cortado exigem, no tipo legal, "para além do dolo do tipo, a intenção de produção de um resultado que, todavia, não faz parte do tipo de ilícito". Cf: JORGE DE FIGUEIREDO DIAS, *Direito Penal*, ob. cit., p. 444

[71] PEDRO SOARES DE ALBERGARIA/PEDRO MENDES LIMA, *O Crime de Detenção de Pseudopornografia Infantil — Evolução ou Involução?* In Revista JULGAR - N.º 12 (especial) – 2010, p. 200

armazenados num computador sob sua responsabilidade ou aos fornecedores de serviços de internet para que estes ofereçam dados dos subscritores.

Por último neste segundo capítulo temos a terceira secção que se ocupa das regras para estabelecer a jurisdição/competência territorial (art. 22.º). Estabelece-se no art. 22.º que "cada parte deverá adotar as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente à prática de qualquer infração penal". Assim, cada Estado terá que ser capaz de criar disposições legais para chamarem a si e aos seus tribunais a competência para a prossecução penal independentemente do local da prática dos factos.

C) Cooperação Internacional

No capítulo III temos presentes as regras para a cooperação internacional. Prevê-se logo no art. 23.º as regras gerais para que as partes cooperarem o mais possível entre si no que concerne à investigação ou ao próprio procedimento criminal das infrações previstas na convenção. A extradição encontra-se no art. 24.º. Podemos, desde já, avançar que, aquando da ratificação, Portugal fez uma reserva nos termos do n.º5 do art. 24.º. Tal encontra-se disposto na Resolução da Assembleia da República n.º 88/2009 que aprova a CCiber, adotada em Budapeste em 23 de novembro de 2001, no seu art. 2.º[72]

Na secção 2 temos disposições específicas para que possa ser possível uma ação concertada e eficaz relativamente às infrações cometidas. No art. 29.º temos a possibilidade de uma parte poder solicitar à outra a conservação expedita de dados "desde que manifeste a intenção de vir a fazer-lhe um pedido formal de assistência para realização de uma busca, apreensão ou diligência similar. Nesse caso, o Estado requerido deverá tomar todas as medidas necessárias à preservação daqueles dados, com respeito pela sua própria lei nacional"[73]. No art. 30.º temos a prevista a divulgação expedita de dados de tráfego conservados e no art. 31.º temos a possibilidade de auxílio mútuo para o acesso a dados

[72] Prevê-se, neste art., o seguinte: "*Portugal não concederá a extradição de pessoas: a) Que devam ser julgadas por um tribunal de exceção (...); b) Quando se prove que são sujeitas a processo que não oferece garantias jurídicas de um procedimento penal que respeite (...) direitos do homem, ou que cumprirem a pena em condições desumanas; c) Quando reclamadas por infração a que corresponda pena ou medida de segurança com carácter perpétuo. Portugal só admite a extradição por crime punível com pena privativa da liberdade superior a um ano. Portugal não concederá a extradição de cidadãos portugueses. Não há extradição em Portugal por crimes a que corresponda pena de morte segundo a lei do Estado requerente. (...) .*"
[73] PEDRO VERDELHO, *Leis do Cibercrime*…, ob. cit., p. 19

informáticos armazenados. No que concerne ao art. 32.º este prevê o acesso transfronteiriço a dados armazenados num computador. Estes dados localizados no estrangeiro poderão ser publicamente acessíveis ou então, caso não o sejam, dependem de consentimento legal e voluntário da pessoa com legitimidade para divulgar os dados. Prevê-se, ainda, no art. 35.º, a criação de um ponto de contacto *24/7*[74] a "fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infrações penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma eletrónica, da prática de infrações penais"

No quarto, e último capítulo, temos as disposições finais.

2.1. A Lei nº 109/2009 de 15 de setembro- Lei do Cibercrime

Como já sabemos LC transpôs para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, de 24 de fevereiro, relativa a ataques contra sistemas de informação adaptando o direito interno à CCiber. A LC foi antecedida pela LCI (Lei n.º 109/91, de 17 de agosto).

De acordo com a Exposição dos Motivos da Proposta de Lei N.º 289/X/4ª "optou-se por condensar neste diploma todas as normas respeitantes à cibercriminalidade e não por proceder à alteração das várias fontes legislativas sobre a matéria" porque se afigura como a "opção legislativa mais coerente com a tradição portuguesa"

Assim a LC, começa, no seu capítulo I, por definir o seu objeto. Segundo o estabelecido no art. 1.º este diploma "estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico". Esta lei não esquece a definição de conceitos relevantes sendo tal previsto no seu art. 2.º. No capítulo II, art. 3.º a 10.º, encontramos o direito penal material. Temos crimes como: Falsidade informática, Dano relativo a programas ou outros dados informáticos, Sabotagem informática, Acesso ilegítimo, Interceção ilegítima, Reprodução ilegítima de programa

[74] A PJ dispõe de um ponto de contacto disponível 24 horas por dia, 7 dias por semana, para solicitações de cooperação internacional emergentes (criado pelo Artigo 21º da Lei do Cibercrime). O ponto de contacto pode ser contactado por via do endereço contacto24.7@pj.pt. Disponível em: CIBERCRIME – REUNIÃO DE COORDENAÇÃO (ministeriopublico.pt) consultado em 28/03/2021

protegida, Responsabilidade penal das pessoas coletivas e entidades equiparada e a Perda de bens.

Importa atentar no capítulo III (arts. 11.º a 19.º) que prevê as disposições processuais.

Segundo o art. 11.º as presentes disposições processuais aplicam-se aos crimes previstos no seu capítulo II- crimes informáticos *stricto sensu*[75]-, aos cometidos através de meios informáticos e em relação aos crimes que se revele necessário proceder à recolha de prova em suporte eletrónico. Faz-se, contudo, uma ressalva importante: as disposições processuais a seguir enunciadas não são aplicáveis ao disposto nos artigos 18.º e 19.º, isto porque estes mecanismos têm um âmbito de aplicação mais restrito[76] que os demais e apresentam um grau mais elevado de intrusão. Por fim, no n. º2 deste art. 11º, alerta-se para não se deixar de ter em conta a Lei n.º 32/2008, de 17 de julho.[77]

O que este diploma pretendeu, em termos processuais, além da introdução de novos meios de obtenção de prova, foi adaptar o nosso sistema (e meios já existentes) ao digital.

Temos, assim, inseridas "figuras processuais novas"[78], como: Preservação expedita de dados (art. 12.º), Revelação expedita de dados de tráfego (art. 13.º), Injunção para apresentação ou concessão do acesso a dados (art. 14.º), Pesquisa de dados informáticos (art. 15.º), Apreensão de dados informáticos (art. 16.º), Apreensão de correio eletrónico e registos de comunicações de natureza semelhante (art. 17.º). Estes constituem um "regime processual geral"[79]. Os arts. 18.º e 19.º (a Interceção de comunicações e Ações Encobertas respetivamente) traduzem-se num "segundo regime processual de autorização e regulação probatória" e "só a este segundo regime (…) são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem a Lei 109/2009"[80]

---

[75] DANIEL BENTO ALVES, "Uso de Malware em investigação criminal" in *Actualidad Jurídica Uría Menéndez*, nº47, 2017, p. 24

[76] No art. 18.º estabelece-se que a interceção de comunicações apenas é admissível nos crimes previstos na presente lei e nos cometidos através de sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do CPP; O âmbito de aplicação do art. 19.º será abordado no ponto 3.2. do presente capítulo

[77] Esta lei transpôs para a OJ interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações

[78] SÓNIA FIDALGO, "A utilização da inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo" In *A Inteligência Artificial no Direito Penal (Coord. Anabela Miranda Rodrigues)*, 2020, p. 148

[79] AC. TRE 20/1/2015, processo nº 648/14.6GCFAR-A.E1, disponível em www.dgsi.pt

[80] *Ibid.*

Não sendo possível analisar com exaustão todos estas disposições processuais, convocamos o disposto no Ac. do TRL de 22/1/2013, processo nº 581/12.6PLSNT-A.L1-5 relatado por Alda Tomé Casimiro[81], com o qual concordamos, onde é afirmado que "este regime [de obtenção de prova] é perfeitamente entendível e justificável. O que está em causa é a obtenção de prova intangível, que só pode corporizar-se no processo com a intervenção especializada e indispensável dos próprios operadores dos sistemas. Se não fosse estabelecido um regime especial como aquele que está definido no mencionado diploma a investigação dos crimes nele previstos estaria condenada ao fracasso e estes crimes seguramente ficariam impunes".

3. O artigo 19º da LC: Ações Encobertas Digitais

Temos consagrado no art. 19.º da LC a possibilidade de recurso a Ações Encobertas em Ambiente Digital. Tal constitui uma medida inovadora, sem correspondência na CCiber que analisámos. A consagração deste método de obtenção de prova traduz, nas palavras de RAMALHO, o reconhecimento da "necessidade do recurso a métodos de investigação criminal mais agressivos em relação a uma criminalidade que tem beneficiado largamente da ineficácia dos restantes meios disponíveis"[82]. É bastante comum o uso da AE digital em países como os EUA em redes *online* como a *Dark Web*[83] dedicadas ao tráfico de droga, pornografia de menores, pedofilia[84], entre outros, revelando-se extremamente eficaz no combate a esta cibercriminalidade.

---

[81] Disponível em www.dgsi.pt

[82] DAVID SILVA RAMALHO, "Investigação criminal na Dark Web" in *Revista da Concorrência e Regulação*, nº 14/15, abril-setembro 2013, p. 408

[83] Temos que fazer a distinção entre as diferentes "camadas": em primeiro, a *Surface Web* e a *Deep Web*. A primeira corresponde à internet que é, tradicionalmente, livremente acessível através de motores de busca como o Google; a segunda, por outro lado, não é livremente acessível e pode necessitar, para aceder, de palavras-passe ou outras autorizações. No âmbito desta última é necessário distinguir entre *Deep Web* e *Dark Web*. Esta última encontra-se dentro da primeira e ambas se caraterizam pela necessidade de utilização anonimizadores (v.g. *Tor*) para o seu acesso. Cf. KRISTIN FINKLEA, "Dark Web", *Congressional Research Service*, março 2017, pp. 2-4 disponível em: https://sgp.fas.org/crs/misc/R44101.pdf consultado a 11/5/2021

[84] Foi recentemente, em meados de 2020, desmantelada uma rede mundial de pedofilia que operava na *Dark Web* com epicentro na Austrália, sendo identificadas 46 vítimas com idades entre os 16 meses e 15 anos. Estavam em causa a prática de 828 crimes com ligações a Nova Zelândia, EUA, Canadá, Ásia e Europa. Foram detidas 14 pessoas nesta operação. Denota-se, aqui, a magnitude que estas redes criminosas *online* apresentam. Fonte: Polícia desmantela rede mundial de pedofilia com centro na Austrália | Austrália | PÚBLICO (publico.pt) consultado em 12/5/2021

3.1. Conceito de ações encobertas digitais

Podemos desde já afirmar que existem, pelo que estudámos até agora, no nosso OJ, dois tipos de ações encobertas: as "clássicas" previstas no n.º 2 do art. 1.º do RJAE e as realizadas em ambiente informático digital reguladas no art. 19.º da LC.[85]

Se anteriormente definimos o que entendíamos por AE "clássica"[86], agora cabe perceber o que distingue estas das realizadas em ambiente virtual.

Comecemos por afirmar que não encontramos, no nosso ordenamento[87], nenhuma previsão expressa de AE desenvolvida em ambiente digital ou de "agente encoberto digital". A sua admissibilidade e aplicação é voltada de forma analógica para o RJAE[88].

Em linhas gerais, se às AE desenvolvidas em ambiente digital se aplica por remissão ou de forma analógica[89] o previsto no RJAE, podemos afirmar que esta ação consistirá na atuação desenvolvida por funcionário da investigação criminal, ou terceiro que atua sob controlo da PJ, tendo como base/propósito a prevenção e repressão dos crimes enunciados no próprio art. 19.º nas suas alíneas a) e b) do n.º1. Como já sabemos do que estudamos a propósito das AE "clássicas", apenas serão admissíveis condutas de infiltração e já não de provocação[90]. Ambas as modalidades têm outros pontos em comum. Como refere RAMALHO podemos assistir à ocultação (ativa ou passiva) da verdadeira identidade do agente e à interação nas vestes de identidade fictícia com o propósito do ganho de confiança de terceiros. Porém, apesar de algumas semelhanças entre ambas as modalidades, concordamos com o autor quando este conclui pela necessidade de regulamentação específica no âmbito das AE digitais dadas as diferenças relevantes e eventuais insuficiências[91] que o regime clássico pode revelar em relação ao caso particular do ambiente informático.

---

[85] DUARTE RODRIGUES NUNES, *Os meios de obtenção*…, ob. cit., p. 196
[86] Cf. Ponto 2.1. capítulo I
[87] Em sentido inverso temos o OJ Espanhol que estabelece, na Ley de Enjuiciamento Criminal, no seu n.º 6 do art. 282 bis, de forma expressa a figura do "*agente encubierto informático*". Este n.º foi aditado pela Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Disponível em: BOE.es - BOE-A-2015-10725 Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. consultado em 12/5/2021
[88] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 284
[89] *Ibid*., p. 283
[90] Retomaremos de forma mais aprofundada este tema no ponto 5. do presente capítulo
[91] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob.cit., p. 284

Podemos, para apoiar este último raciocínio, elencar algumas notas diferenciadoras[92] entre a AE "clássica" e a AE digital. No mundo virtual, um AE pode desdobrar-se em múltiplas personalidades, ao mesmo tempo, em diferentes espaços virtuais, podendo interagir com variadíssimas pessoas de diferentes pontos do globo, nunca expondo a sua imagem física exercendo tudo isto no seu gabinete correndo muito menos riscos do que o AE que se infiltra fisicamente numa organização criminosa, expondo-se de uma forma muito mais evidente e, muitas vezes, perigosa. Assim estas "diferenças operacionais"[93] revelam a evidente necessidade de regulamentação complementar. A mera remissão para o regime geral pode deixar algumas zonas cinzentas sem resposta pois não abarca em si todas as possibilidades de atuação de um AE no ciberespaço dado que não foi esta a *ratio legis* da criação do RJAE.

3.2. Âmbito de aplicação e requisitos

Nos termos do disposto no art. 19.º da LC pode lançar-se mão da AE digital quando estiver em causa a investigação de: a) crimes previstos nos artigos 3.º a 8.º da LC; b) crimes puníveis com pena de prisão superior a 5 anos e sejam praticados através de sistema informático e c) crimes dolosos, independentemente da pena aplicável, contra a autodeterminação sexual nos casos de ofendidos menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.

Estamos, assim, perante um alargamento ao (já extenso) catálogo de crimes que admitem o recurso a AE estabelecido no art. 2.º do RJAE. Assim, conforme SUSANA AIRES DE SOUSA refere, este alargamento opera em dois sentidos: por um lado, adita novos crimes ao catálogo do regime geral; por outro, admite que a AE seja realizada com recurso a meios e dispositivos informáticos sem que se concretize que meios são admissíveis na realização destas ações[94].

[92] Partimos do exposto por DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., pp. 284-286
[93] *Ibid.* p. 284
[94] SUSANA AIRES DE SOUSA, *Ações Encobertas…* ob.cit., p. 38

Este alargamento é alvo de diversas críticas. DÁ MESQUITA afirma que se ultrapassou "a linha do admissível"[95] ao prever o recurso a este mecanismo (idealmente de caráter excecional, de última *ratio*) para um leque tão extensivo de crimes. Também neste sentido vai DUARTE RODRIGUES NUNES que manifesta a sua estranheza perante o catálogo estabelecido no artigo, "sendo muito mais amplo"[96].

Neste ponto concordamos com ambos os autores parecendo-nos excessivo o alargamento operado pela LC. Acrescentamos, acompanhado SUSANA AIRES DE SOUSA, que acaba por existir um desencontro entre o RJAE e a LC. Tomemos como exemplo os crimes contra a liberdade e autodeterminação sexual: no RJAE exige-se, para se lançar da AE, que o crime seja, em abstrato, punível com uma pena superior a 5 anos ainda que a vítima tenha menos de 16 anos; na LC, ao invés, não se exige o requisito da pena aplicável para fazer uso de AE digital; a AE digital pode ser usada em qualquer crime doloso contra a liberdade ou autodeterminação sexual de menor (de 18 anos); a AE física só pode ser usada quando em causa esteja um crime sexual contra menor de 16 anos punível com pena superior a 5 anos[97]. Parece-nos não existir qualquer lógica e fundamento para esta discrepância.

No que aos requisitos[98] diz respeito temos que atentar no RJAE e no disposto no seu art. 3.º. Como explorámos acima, temos, no n.º1, previsto o princípio da proporcionalidade. Assim, o recurso a este mecanismo tem que se revelar indispensável para a descoberta da verdade e para a obtenção de prova regendo a ideia de que seria impossível ou muito difícil a sua obtenção de outra forma. Temos subjacente a indispensabilidade da diligência. Ademais, terá que existir uma suspeita fundada acerca da prática de um dos crimes do catálogo. A AE tem caráter de *última ratio* e, como tal, só se poderá recorrer a este método de obtenção de prova quando os outros menos lesivos não forem idóneos à satisfação do resultado que se pretende atingir.

Além do respeito por tudo isto, a realização de uma AE, no âmbito do inquérito, depende da prévia autorização do magistrado do MP sendo obrigatória a comunicação ao JIC, considerando-se a mesma validada caso não seja proferido despacho de recusa nas 72hs seguintes.

---

[95] PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, 2010, pp. 125 e ss
[96] DUARTE RODRIGUES NUNES, O*s meios de obtenção …* ob.cit., p. 206
[97] SUSANA AIRES DE SOUSA, *Ações Encobertas*… ob. cit., p. 38 nota de rodapé 11
[98] DUARTE RODRIGUES NUNES, *Os meios de obtenção*… ob. cit., pp. 205-209

3.3. Identidade fictícia *online*

De acordo com o disposto no art. 5.º do RJAE o AE pode atuar ao abrigo de identidade fictícia atribuída por despacho do Ministro da Justiça mediante proposta do Diretor Nacional da PJ. Refere-se, ainda, que esta identidade pode ser utilizada por seis meses, renováveis, estando o agente autorizado a fazer uso dela "quer no exercício da concreta investigação quer genericamente em todas as circunstâncias do tráfico jurídico e social".

O que se tem em vista com a atribuição desta identidade fictícia será a proteção do agente permitindo-lhe atuar ao abrigo de outra identidade oficial (ser-lhe-ão facultados documentos que atestem esta identidade como Cartão de Cidadão, conta bancária, "criação" de uma nova família e círculo de amigos, criação de páginas online que atestem a identidade e aparência criminosa do agente,…).[99]

O que agora pretendemos perceber é em que medida a utilização de identidade fictícia se revela essencial no decurso da AE digital ou se, por outro lado, não acrescenta grande utilidade para o sucesso da mesma. Em contexto digital, a regra é a ausência de identificação, ao invés do que ocorre em ambiente físico. A identificação é uma exceção dado os frequentadores das redes criminosas digitais se identificarem através de *usernames* ou *nicknames* (estes raramente retratam a sua identidade verdadeira), sendo toda a comunicação feita através da utilização destes nomes de utilizador sem haver conhecimento da aparência física ou localização da pessoa com quem se comunica. Como tal, os agentes policiais não serão alheios a esta tendência e adotarão, também eles, uma identidade fictícia através de um *username* ou *nickname* que não os identifique. Conforme RAMALHO observa, a interação *online per si* não implica um risco acrescido para os agentes que justifique o uso de identidade fictícia uma vez que, à partida, os suspeitos não terão qualquer elemento identificativo do agente.[100] Neste ponto em particular, o AE "clássico" corre muito mais riscos uma vez que o contacto é pessoal.

Contudo consideramos que a sua adoção pode revelar-se bastante proveitosa. Caso se faça uso desta possibilidade, terá sempre que existir uma prévia e necessária autorização

[99] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., pp. 304-305; DUARTE RODRIGUES NUNES, *Os meios de obtenção*… ob. cit., pp. 213
[100] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 305

da autoridade judiciária competente na qual deverá constar que o agente irá, durante a sua atuação, criar uma identidade fictícia fazendo-se referência expressa aos limites a ser respeitados e, principalmente, que identidade irá ser adotada de modo a evitar que os agentes criem outras identidades fictícias não autorizadas. Julgamos ser, inclusive, a opção mais segura para o próprio sucesso da AE. O facto de existir um despacho que autorize o agente a utilizar determinada identidade fictícia oferece, em nossa perspetiva, segurança à própria AE pois baliza-se o concretamente admissível de forma a que se evitem provocações e tentativas de enganar o suspeito através da criação de outros *usernames* que servem apenas esse propósito ardiloso. Na sua criação é de evitar os nomes excessivamente sugestivos e deve ser prevista a possibilidade de se fazer uso de fotografias de outrem para criação de um perfil falso.[101] Deve também ser estipulado um limite máximo para a utilização dessa identidade. Sempre que não existam impedimentos o agente pode, inclusive, fazer uso de um *username* de um terceiro que havia pertencido ao meio criminoso que se investiga desde que as suas credenciais sejam voluntariamente ou legalmente obtidas. Contudo esta última possibilidade revela-se discutível porque ao utilizar um terceiro ("*um civil- um homem de confiança em sentido restrito-[…]*"[102]) que os suspeitos já conhecem e em quem já têm confiança proporciona, por um lado, acesso a informações privilegiadas e, por outro, uma atuação particularmente desleal por parte do AE devendo existir circunstâncias excecionais que justifiquem este engano acrescido[103]. Assim, deverá ser admitido o recurso a estes terceiros nos casos em que é impossível a infiltração do agente policial naquele meio criminoso sendo a única solução o aproveitamento de alguém que já se encontra inserido no mesmo[104] ou quando esse terceiro tem conhecimentos técnicos que permitem a infiltração em áreas que o AE não conseguiria ter acesso[105].

[101] *Ibid.*, p. 306
[102] *Ibid*. p. 298
[103] *Ibid.* p. 306
[104] *Ibid.* p. 298
[105] *Ibid*. p. 299

4. A Ação Encoberta Digital e o conflito com as Finalidades do Processo Penal

São tradicionalmente atribuídas três finalidades ao processo penal[106]: a realização da justiça e a descoberta da verdade material; a proteção perante o Estado dos DF's dos cidadãos; e o restabelecimento da paz jurídica posta em causa com o cometimento do crime. Estas finalidades podem, por vezes, conflituar entre si.

Podemos afirmar que a descoberta da verdade material é "preordenada à realização da justiça pela via da perseguição, identificação e punição dos agentes do crime"[107] constituindo um "dever ético e jurídico"[108]. Assim, a realização da justiça estará assegurada quando o Direito for capaz de se aproximar o mais possível daquilo que efetivamente aconteceu[109]. Para que seja aferida a verdade material e, consequentemente, realizada a justiça, o percurso a percorrer tem de ser pautado pela utilização de "meios processualmente admissíveis e por forma a assegurar a paz jurídica dos cidadãos"[110] tendo que se operar uma "concordância prática das finalidades em conflito"[111] com limite na dignidade da pessoa humana, na inviolabilidade da vida privada, do domicílio, da correspondência e das telecomunicações[112]. Assim, o direito processual penal configura-se como um "sistema construído com fundamento e limite na dignidade da pessoa humana e, em particular, na integridade pessoal do arguido"[113]. Existem, portanto, áreas intransponíveis e inacessíveis para a obtenção de prova. Conforme observa RAMALHO, caso a base de condenação de um arguido seja construída com fundamento no recurso a meios processualmente inadmissíveis (entenda-se violadores de DF's do arguido ou da dignidade da pessoa humana- *v.g.* recurso a tortura) terá de se abdicar dessa mesma condenação[114] pois não podemos

---

[106] MARIA JOÃO ANTUNES, *Direito Processual Penal*… ob. cit., p. 14
[107] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova*... ob. cit., p. 81
[108] AC. TC n.º 607/2003 de 5 de dezembro de 2003, Proc. n.º 594/03, disponível em: www.tribunalconstitucional.pt
[109] SUSANA AIRES DE SOUSA, Neurociências e Processo Penal: Verdade Ex Machina? In *Estudos em Homenagem ao Prof. Doutor Manuel da Costa Andrade*, Volume II, 2017, p. 884
[110] Preâmbulo CPP: exposição dos motivos, parte II, ponto 5.
[111] MARIA JOÃO ANTUNES, *Direito Processual Penal*… ob. cit., p. 15
[112] Cf. Ac. TC nº 607/2003 em que se afirma: "*A verdade material não pode conseguir-se a qualquer preço: há limites decorrentes do respeito pela integridade moral e física das pessoas; há limites impostos pela inviolabilidade da vida privada, do domicílio, da correspondência e das telecomunicações, que só nas condições previstas na lei podem ser transpostos"*
[113] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob. cit., p. 182
[114] *Ibid*., p. 185

procurar a verdade a todo o custo. Obviamente que não podemos cair em extremos e existirá sempre ingerência nos DF's do individuo. Conforme sublinha RAMALHO, nenhum sistema processual penal eficaz se constrói "sem qualquer ingerência nos direitos fundamentais dos cidadãos"[115]. Daí que se tenha afirmado pela necessidade da concordância prática entre as finalidades em conflito. Assim, é necessário "relativamente a cada problema concreto uma mútua compressão das finalidades em conflito, de forma a atribuir a cada uma a máxima eficácia possível: de cada finalidade há-de salvar-se, em cada situação, o máximo conteúdo possível, otimizando-se os ganhos e minimizando-se as perdas axiológicas e funcionais."[116] O exercício a ser feito passará por uma análise casuística colocando de um lado da balança os interesses do Estado (a realização da justiça e a descoberta da verdade material) e, do outro, os DF's do visado. Conforme afirma CONDE CORREIA "o direito processual é assim um instrumento privilegiado de agressão dos direitos, liberdades e garantias individuais e, ao mesmo tempo, um meio indispensável para a sua proteção"[117]

Para garantir que em matéria probatória a obtenção e posterior valoração seja feita através de meios processualmente admissíveis que não lesem DLG's temos alguns limites/obstáculos à descoberta da verdade material.

4.1. Os limites à descoberta da Verdade Material

A) Proibições de Prova

No que às proibições de prova diz respeito, comecemos por uma introdução relativamente ao que se entende por Prova. Socorremo-nos do estabelecido no art. 341.º do CC que encerra em si o seguinte: "as provas têm por função a demonstração da realidade dos factos". Segundo o CPP, no seu art. 124.º, serão objeto da prova "todos os factos juridicamente relevantes para a existência ou inexistência do crime". Assim, definimos a prova como tudo aquilo que é recolhido no decorrer da investigação que seja essencial para

[115] *Ibid.* p. 183
[116] Ac. STJ de 12/3/2008, processo n.º 08P694 disponível em www.dgsi.pt
[117] JOÃO CONDE CORREIA, *Contributo para a análise da inexistência e das nulidades processuais*, 1999, p. 191

demonstrar a realidade[118] de determinados factos "alegados em juízo"[119] que irão guiar e habilitar o julgador a proferir uma decisão sobre essa determinada factualidade

Como já vimos, entre a descoberta da verdade material e a proteção dos DF's poderão existir alguns conflitos isto porque a busca pela verdade material não pode atropelar os DF's que terão sempre que ser protegidos.

O regime de proibições de prova destina-se exatamente a balizar as linhas intransponíveis. Estas linhas estão previstas nos arts. 32.º/8 da CRP e 126.º do CPP.

Rezam os artigos supramencionados o seguinte:

"*Artigo 32.º (Garantias de processo criminal)*

[…]

8. São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações"

"Artigo 126.º Métodos proibidos de prova

1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas.

[…]

3. Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular."

Mas o que podemos entender como proibições de prova? Conforme refere COSTA ANDRADE citando GÖSSEL podemos definir as proibições de prova como "barreiras colocadas à determinação dos factos que constituem objeto do processo"[120]. Ou seja, funcionam como limites/barreiras à descoberta da verdade material.

[118] Dicionário Jurídico, *Vol II Direito Penal e Direito Processual Penal,* 2009, pp. 421 e 422; Dicionário da Língua Portuguesa Contemporânea da Academia das Ciências de Lisboa, II Vol., 2001, p. 2992
[119] Enciclopédia Fundamental Verbo, Editor: Verbo, 1989, p. 1285
[120] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova*... ob. cit., p.83

Podemos distinguir, dentro das proibições de prova, dois conceitos: as proibições de produção de prova e as proibições de valoração de prova[121]. As primeiras poderão ser i) proibições de temas de prova, ii) proibição de métodos de prova, iii) proibição de meio de prova e iv) proibições de leitura de protocolos[122]. No que concerne aos primeiros, estão em causa factos que não podem ser objeto de prova. Os segundos tem que ver com meios de prova que não poderão ser utilizados. O terceiro liga-se ao facto de não poderem ser empregues certos meios de recolha de prova. Já as proibições de valoração poderão ser proibições dependentes e independentes sobressaindo, nestas últimas, as proibições de valoração de matriz constitucional. Serão dependentes quando a proibição de prova dependa "da verificação prévia de uma proibição de prova"[123] ou então poderão ser independentes quando não pressupõem "a verificação de qualquer vício na produção de prova" sendo o cerne da questão de matriz constitucional e, como tal, deve passar-se "para segundo plano" a prossecução penal porque caso não se faça DF's serão afetados[124]. Temos como exemplo desta última hipótese o caso que deu origem ao Ac. do TC nº 607/2003[125]. Este Acórdão teve como base a apreensão de um diário íntimo de um arguido no âmbito do processo Casa Pia e é muito importante nesta temática, conforme observa MARIA JOÃO ANTUNES, porque coloca de um lado a necessidade de descoberta da verdade material e do outro a proteção dos DF's[126]. Questiona-se até que ponto se pode ir na intromissão dos DF's para descobrir a verdade material. Assim, este Acórdão oferece-nos uma máxima que consideramos dever ser o norteador de toda a investigação criminal afirmando-se: "Existe um dever ético e jurídico de procurar a verdade material. Mas também existe um outro dever ético e jurídico que leva a excluir a possibilidade de empregar certos meios na investigação criminal". Ou seja, a verdade material tem sempre que ser obtida através de meios processualmente válidos que não atentem contra o princípio da dignidade humana (art. 1.º da CRP).

Deste modo, estamos perante uma proibição de prova quando, na obtenção da mesma, foram lesados DF's (n.º 8 do art. 32.º 1.ª parte da CRP e n.º 1 do art. 126.º do CPP)

[121] *Ibid*., p. 90
[122] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob. cit., p.191
[123] *Ibid.*
[124] *Ibid.*
[125] Disponível em: www.tribunalconstitucional.pt
[126] MARIA JOÃO ANTUNES, *Direito Processual Penal*… ob. cit., p. 16

ou não foram respeitadas certas formalidades processuais (n. º8 do art. 32.º 2.ª parte da CRP e n.º 3 do art. 126.º do CPP).

.

5. O agente provocador digital: dificuldades na delimitação desta figura

Se anteriormente neste estudo analisámos a linha ténue que separa a infiltração da provocação em ambiente físico, muito mais difícil será a delimitação no ciberespaço.

DUARTE RODRIGUES NUNES na senda ALVES MEIREIS estabelece uma estrutura tripartida na definição dos atores das AE digitais[127]. Começa por definir o AE em plano digital como alguém cuja atividade poderá passar pelo " «patrulhamento» de sítios na internet, *chats* ou *newsgroups* abertos ou acedidos com o consentimento de um dos participantes, de redes P2P e outras «zonas de risco» do Mundo virtual"[128], pela criação de uma página na internet de forma a identificar suspeitos da prática de um determinado crime ou mesmo a participação do agente em *chats, sites, blogs* ou fóruns que sejam de livre acesso desde que não tenha interação com os demais participantes, é um mero observador do conteúdo que vai sendo partilhado. No que ao agente infiltrado diz respeito, o autor define-o como aquele que frequenta sítios na internet, ao abrigo de identidade fictícia ganhando confiança dos visados, mantendo-se a par dos acontecimentos e da execução dos factos podendo interagir com os outros participantes, mas sem nunca os determinar ao cometimento de infrações[129]. Não é esquecido o agente provocador que o autor define como aquele que "convence outrem a cometer um crime que, não fosse a atuação do agente provocador, jamais cometeria"[130] ou seja, existe um nexo de causalidade entre a conduta do agente provocador e a do provocado dado que este último só pratica o ilícito por força da provocação do primeiro.

Como já havíamos afirmado, seguindo a visão de RAMALHO, parece-nos pouco pertinente esta distinção[131] entre AE e Agente Infiltrado sendo de criticar veemente o

[127] DUARTE RODRIGUES NUNES, *Os meios de obtenção*… ob. cit., pp. 197-199
[128] *Ibid*. p. 197
[129] *Ibid*. p. 199
[130] *Ibid.*
[131] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 289

entendimento de enquadrar o AE como mero observador dos ilícitos que vão sendo cometidos.

Por sua vez, seguindo o ensinamento de ZARAGOZA TEJADA podemos enunciar três elementos característicos da figura do AE comuns em todas as definições no direito comparado: a infiltração numa rede criminosa, a ocultação da verdadeira identidade e a infiltração é efetuada por um agente policial[132]. Com base nestas coordenadas, o autor elabora um conceito de AE digital traduzindo-se este num "miembro de las Fuerzas y Cuerpos de Seguridad del Estado que, voluntariamente, y mediando la correspondiente resolución judicial, se infiltra en la Red con el fin de obtener información sobre práticas delictivas producidas a través de la misma y la identificación de sus autores y/o partícipes. Dicha infiltración se produciria a través del mecanismo de ocultación de la verdadeira identidade, a fin de ganarse la confianza de un grupo de delicuentes obteniendo, com ello, pruebas suficientes de los hechos ilícitos perpetrados por los mismos"[133] Assim, com inspiração neste conceito, podemos definir o AE do ciberespaço como um funcionário da investigação criminal (PJ) que se infiltra numa rede criminosa online com o propósito de obter informações sobre crimes praticados (ou em vias de serem praticados) e identificação dos respetivos autores. Esta infiltração é levada a cabo sob proteção de identidade fictícia (através da adoção de *usernames* e *nicknames*) de forma a que o agente ganhe a confiança dos criminosos e, também, recolha provas suficientes dos crimes por eles praticados.

Distinto será o agente provocador. Como já sabemos, este agente cria o próprio crime, cria uma intenção criminosa até então inexistente. Esta conduta, por tradição, é reconduzida à figura dos meios enganosos nos termos da alínea a) do n. º2 do art. 126.º do CPP. Porém, como SUSANA AIRES DE SOUSA afirma, para que a provocação seja um meio enganoso, entre a conduta do agente provocador e a conduta do provocado tem que existir um nexo de causalidade. Noutras palavras, diz a autora que "é porque o provocado está enganado quanto à qualidade do agente policial que ele pratica o crime ou fornece informações e provas que vão incriminá-lo"[134].

Num plano mais prático e transportando estes entendimentos para o mundo virtual: quando é que estaremos perante uma provocação no domínio *online*? Podemos elencar

[132] JAVIER ZARAGOZA TEJADA, El Agente Encubierto "online" in *Investigación tecnológica y derechos fundamentales: comentarios a las modificaciones introducidas por la ley 13/2015***,** 2017, p. 329
[133] *Ibid*., pp. 329-330
[134] SUSANA AIRES DE SOUSA*, Agent Provocateur…,* ob. cit., p. 1233

algumas questões práticas de modo a percebermos melhor o que podemos enquadrar neste conceito. Iremos tomar como ponto de referência os crimes de pornografia de menores ou pedofilia *online* que são, como acima se referiu, alguns dos crimes que mais justificam o recurso a uma AE digital.

Ao proceder-se à infiltração num *site*, fórum, *chat* ou outro com fins ilícitos, muitas vezes o próprio agente pode ser "posto à prova". Os criminosos, para confiarem no AE, podem solicitar, *v.g.,* o envio de material ilícito- frequente nas redes criminosas que se dedicam a pornografia infantil onde, para ter acesso às mesmas, é necessário o prévio envio de material pornográfico. Imaginemos, seguindo este exemplo, o seguinte: ao tentar entrar numa rede em que se partilham conteúdos de teor pornográfico envolvendo menores, é solicitado ao agente o envio de um vídeo/fotografia para poder aceder ao *website*. Podemos pensar no caso emblemático *Wonderland Club*[135], onde para ter acesso a esta rede era necessária a disponibilização de dez mil fotos de conteúdo pornográfico de menores.

Será que esta disponibilização é permitida? Será que o ceder de tal conteúdo comporta uma provocação? A propósito desta temática, BUENO DE MATA, acentua que acima de toda a investigação criminal está sempre a "protección de la infancia"[136]. Entendimento com o qual concordamos. Assegurar a proteção de crianças e adolescentes de eventuais abusos e exploração sexuais afigura-se essencial nestes contextos. Caso se proceda à disponibilização deste conteúdo por parte do AE, imperativo será proteger a imagem dos menores em causa (*v.g.,* através da distorção da imagem, da criação de um vídeo com crianças virtuais tridimensionais ou através do uso de inteligência artificial e de programas informáticos específicos para o efeito)[137].

No que toca conceito de conduta provocadora, o autor supracitado refere que esta passa pelo "inducir a realizar una determinada acción ilícita a alguién no tenía la intención de hacerlo"[138] ou seja, a disponibilização por parte do AE de um vídeo pornográfico de menores (atendendo-se, obviamente, ao que referimos acima a propósito da sua proteção)

---

[135] Para mais sobre a investigação: Technological level of Wonderland network shocked all investigators (irishtimes.com) consultado a 11/5/2021

[136] FEDERICO BUENO DE MATA, *El Agente Encubierto en Internet…* ob cit., p. 303; No mesmo sentido admitindo a possibilidade de ser concebível o envio deste conteúdo desde que autorizado pelos representantes legais do menor ou através de técnicas de anonimização dos menores. DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., pp. 307-308

[137] Ideia semelhante foi levada a cabo no Caso *Sweetie* onde se criou uma criança virtual que abordava predadores sexuais. Para aprofundamento do tema: Primeira condenação no caso Sweetie, a criança virtual abordada por predadores sexuais | Crianças | PÚBLICO (publico.pt) consultado a 30/4/2021

[138] FEDERICO BUENO DE MATA, *El Agente Encubierto en Internet…* ob cit., p. 304

com o propósito de aceder à rede criminosa num *website* dedicado apenas à troca deste conteúdo, não iria criar a intenção criminosa, dado que esta já existe previamente, já foram trocados muitos outros vídeos antes do acesso por parte do AE. A disponibilização adicional de conteúdo não irá criar uma nova intenção criminosa, os intervenientes no *website* já têm a sua intenção criminosa formada praticando os factos independentemente da atuação do AE[139]. Este ato terá o propósito de ganho de confiança naquele primeiro contacto em que se tenta aceder à rede, algo verdadeiramente essencial para que a investigação prossiga. Podemos trazer à discussão o facto do AE ser autor imediato[140] do crime de pornografia de menores. Aqui RUI PEREIRA afirma que ao AE se encontra vedada a prática de ilícitos, admitindo-se apenas na modalidade de comparticipação.[141] Já para EDUARDO MAIA COSTA o AE pode praticar ilícitos desde que tal se revele necessário para a prossecução do fim visado pela ação, o grau de ofensividade ser o menor possível e não se incluam ofensas pessoais[142]. Conforme RAMALHO consideramos que a conciliação de ambas é o melhor caminho[143]. Porém, também particularizamos, na mesma linha do autor, o facto do bem jurídico protegido pertencer a um menor[144]. Neste cenário, consideramos que a solução passa pelo que referimos *supra* e deve fazer-se uso de programas informáticos que protejam a imagem das crianças.

Ainda na senda da infiltração em redes criminosas envolvendo menores, imaginemos a hipótese de um agente que se infiltra num *website, chat* ou fórum criminoso em que apenas requer o registo prévio para ter acesso ao mesmo (e já não o envio de conteúdo como acima se equacionou) e, nesse processo, opta por um *username* ou *nickname* sugestivo? Pensemos na utilização de um *nickname* como "*12yearoldgirl*"[145] num *website*

[139] Exclui-se, portanto, o nexo de causalidade entre a atuação do AE e a conduta dos visados pela ação. SUSANA AIRES DE SOUSA, *Agent Provocateur*.., ob. cit., p. 1234

[140] É autor imediato quem executa o facto pelas suas próprias mãos "em termos de preencher na sua pessoa a totalidade dos elementos objetivos e subjetivos do ilícito típico e deter por isso, (…), o domínio da ação" JORGE FIGUEIREDO DIAS, *Direito Penal*, ob. cit., p. 905

[141] RUI PEREIRA, O "agente encoberto" na ordem jurídica portuguesa in *Medidas de Combate à Criminalidade Económico-Financeira*, 2004, p. 32 *apud* DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 307

[142] EDUARDO MAIA COSTA, *Ações Encobertas (Alguns problemas, algumas sugestões)* in Estudos em Homenagem ao Conselheiro Artur Maurício, 2014, p. 365 *apud* DAVID SILVA RAMALHO, Métodos Ocultos…, ob. cit., p. 307

[143] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 307

[144] *Ibid.* p. 308

[145] Exemplo avançado por DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 296

utilizado essencialmente por pedófilos. Será que a utilização deste *nickname* sugestivo pode ser subsumível a uma atuação provocadora? Conforme RAMALHO observa, a utilização deste *username* pode ser um convite à interação, funcionando como uma solicitação de contacto para a prática de ilícitos[146]. Como já sabemos, é comum serem adotados os mais variados *usernames*, o que não nos parece admissível será a utilização de uma identificação extremamente sugestiva e convidativa que leve outros a interagir com o agente por causa daquele nome. Pensemos na hipótese acima levantada: a utilização de um *username* com aquele teor poderá levar a que pedófilos encetem conversações com o agente simplesmente porque foram "atraídos" pela sua identificação. Se ao invés tivesse adotado uma identificação com caráter mais neutro, talvez tal não acontecesse (ou não de uma forma imediata).

Ainda no âmbito desta problemática, ZARAGOZA TEJADA alerta para uma prática levada a cabo pelos órgãos policiais espanhóis que consideramos de extrema importância abordando o tema a propósito de uma sentença do Supremo Tribunal n.º 767/2007 de 3 de outubro[147]. O que estava em causa era a utilização, por parte um agente da Guardia Civil, de um *nickname* ("rata") num site dedicado ao envio de conteúdo pornográfico envolvendo menores. Um indivíduo que fazia parte dessa rede enviou fotografias e outros conteúdos deste teor ao agente. Na manutenção destes contactos o agente teve conhecimento da existência de uma rede ("*la gran família*") onde vários adultos encetavam encontros sexuais com os filhos menores. A particularidade deste caso reside no facto de, só depois do conhecimento, por parte do agente, desta "*la gran familia*", é que foi desenvolvida a AE propriamente dita, requerendo-se a respetiva autorização ao JIC. Estamos perante uma atuação prévia à própria AE ("ciberpatrullaje[148]") que tem o propósito de reunir indícios suficientes[149] que justifiquem o posterior recurso à AE[150]. Assim, estamos perante um caso onde o agente policial acedeu a um site publicamente acessível, registando-se e procedeu à monitorização da atividade antes sequer de ser iniciada uma AE. Traduz-se numa

[146] *Ibid.*
[147] Disponível em: STS 767/2007, 3 de Octubre de 2007 - Jurisprudencia - VLEX 31969904 consultado a 30/5/2021
[148] Trata-se de uma investigação com vista à prevenção de práticas delituosas feita em páginas publicamente acessíveis (*v.g.* redes sociais) sendo uma técnica perfeitamente válida sem exigência de requisitos especiais. JAVIER ZARAGOZA TEJADA, *El Agente Encubierto "online",* ob. cit., pp. 335- 339
[149] Entende-se que estamos perante indícios suficientes sempre que a condenação se mostrar mais provável do que a absolvição (art. 283º/1 e 2 CPP).
[150] JAVIER ZARAGOZA TEJADA, *El Agente Encubierto "online*", ob. cit., pp. 337-339

ação com fins preventivos com o propósito de recolher indícios suficientes que lhe permitam, posteriormente, pôr em prática a AE propriamente dita. Consideramos uma conduta legítima e de extrema utilidade para a investigação criminal. Ao ser feita a monitorização destes sítios da internet potencialmente criminosos, fora do contexto das AE, pode prevenir-se a prática futura de inúmeros ilícitos e descobrir-se a prática de muitos outros. Esta atuação tem espelho no mundo físico na atividade do agente à paisana que por exemplo se desloca a um café onde sabe que é frequente tráfico de drogas.

Imaginemos, agora, os casos em que o agente decide ter uma conduta ativa e encetar, ele próprio, conversações privadas com os visados depois de se aperceber que estes disponibilizaram vários conteúdos ilícitos no *website* que este se encontra a patrulhar? Aqui já estaremos perante contactos feitos de forma privada. Nestes cenários é inequívoca a necessidade de recorrer ao AE digital[151] dado estarmos perante conversações com pessoas concretas, feitas de modo privado, sendo que o agente atua, como se disse, ao abrigo de uma identidade fictícia apresentando-se como um criminoso tentando entrar no círculo de confiança do visado. Como tal, terão que ser verificados todos os requisitos[152] base de recurso à AE. O que não se pode verificar é uma incitação à prática de crimes por parte do agente nesse âmbito de conversa particular, como por exemplo uma solicitação por parte do agente ao visado de envio de material ilícito com o propósito de o perseguir criminalmente.

6. A necessidade de um regime específico para o ambiente digital

Das hipóteses expostas constatamos que a delimitação de fronteiras entre o AE e o provocador se revela uma tarefa particularmente difícil em ambiente digital. Mas não só neste ponto particular se sentem dificuldades. A remissão expressa da LC para o RJAE parece esquecer todas as especificidades[153] que o ambiente digital tem na sua essência. Não nos parece viável a solução atual que nos remete simplesmente para a aplicação de um

[151] *Ibid*., p. 336
[152] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 298
[153] Nas palavras de DIAS RAMOS que acompanhamos: "O legislador continua ainda a olhar para a criminalidade informática, que pode ser muito grave, inclusive com atos terroristas, com olhos de equiparação entre duas realidades que são bem distintas" ARMANDO DIAS RAMOS, *Prova digital em Processo Penal: O Correio Eletrónico*, 2017, p. 157

regime pensado para AE físicas. Existem particularidades que podem ficar sem proteção por insuficiência[154] do regime. Devia o legislador, aquando da criação da LC e admissibilidade do uso do AE digital, ter densificado o conceito do AE digital, requisitos, limites, meios e modos de atuação, criando normas que se adaptassem ao mundo digital. E, sobretudo, não admitir o uso deste mecanismo num leque tão alargado de ilícitos pois desvirtua o próprio caráter de *última ratio* da AE. Por todas as dúvidas que pairam, a opção por uma base legal específica para este novo método de obtenção de prova no domínio digital onde fossem aprofundados os aspetos referidos supriria algumas das lacunas ainda observadas. O legislador olha para a criminalidade informática, que pode ser muito mais grave que a "criminalidade física" com olhos de equiparação entre duas realidades que são bem distintas. Revela-se, na nossa perspetiva, essencial uma evolução legislativa que passe pela regulamentação específica, clara e precisa das AE digitais por todas as especificidades que analisámos e pelas lacunas que se observam na prática. Apenas com uma nova tutela para o digital se resolverão as lacunas que se verificam. Já é bastante percetível, por tudo o que temos vindo a estudar, que a adaptação do regime já existente a novas realidades cria ainda mais problemas do que aqueles que aparentemente pretende solucionar. Fazendo uso das palavras de CONDE CORREIA "uma lei mal concebida provoca mais danos à administração da justiça do que uma boa lei *ab initio* insuficiente"[155]. É necessária criatividade legislativa. Perceber as falhas e deficiências da LC para que estas sejam supridas e alteradas de forma a que a justiça penal de facto ocorra.

[154] Acompanhamos RAMALHO quando este afirma "a redução de uma realidade complexa a um núcleo simples, vago e abstrato (…) é suscetível de revelar insuficiências" DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob. cit., p. 284

[155] JOÃO CONDE CORREIA, *Prova digital: as leis que temos e a lei que devíamos ter*, RMP 139, Ano 35, julho/setembro 2014, p.59

CAPÍTULO III. Da prova obtida pelo agente encoberto digital

1. Prova digital: algumas notas, conceito e caraterísticas

Comecemos o presente capítulo por algumas notas introdutórias que se afiguram pertinentes para o estudo do tema que agora nos ocupa. Em primeiro lugar, referir que a temática da prova digital é verdadeiramente essencial nos tempos atuais por força de todas as inovações que temos vindo a sublinhar. Em segundo, esta problemática encontra-se regulada, no nosso ordenamento, em três diplomas: o CPP, a Lei n.º 32/2008 (Conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas) e a Lei n.º 109/2009 (LC). Em terceiro lugar e relacionado com este último aspeto, esta regulação da prova digital em três diplomas leva a que acabemos por cair num verdadeiro "pântano prático e, sobretudo, normativo"[156] levando a diversas incongruências, zonas cinzentas e ausência de resposta prática. Iremos no ponto seguinte (ponto 1.2.) debruçarmo-nos criticamente sobre esta confusão legislativa e problemas que daqui resultam.

Por agora, iremos abordar o que entendemos por prova digital e as suas caraterísticas próprias que exigem que seja tratada com particularidade.

No que diz respeito ao conceito propriamente dito, temos que começar por referir que na legislação portuguesa não encontramos qualquer definição de "prova digital". Temos apenas referência na LC à "prova em suporte eletrónico" (arts. 1.º, 11.º/1/c, 18.º/1/b, 20.º). Mas serão estes conceitos sinónimos? Sucede por variadas vezes os conceitos serem utilizados como sinónimos o que pode levar a confusão.[157] Assim, STEPHEN MASON E BURKHARD SCHAFER definem a prova eletrónica como todos os dados que são criados, manipulados, armazenados ou comunicados por qualquer dispositivo, computador, sistema informático ou transmitidos por um sistema de comunicação que têm potencial de tornar a explicação factual de uma das partes mais provável ou menos provável do que aquilo que seria sem a prova.[158] Já no que ao conceito de prova digital diz respeito, DIAS RAMOS

---

[156] JOÃO CONDE CORREIA, *Prova digital: as leis que temos*…, ob.cit., p. 30

[157] "*The term 'electronic evidence' is used widely, but it is commonly used to denote digital evidence, which adds to the confusion*" STEPHEN MASON, *Internacional Electronic Evidence*, Londres: British Institute of Comparative Law, 2008, p. xxxvi

[158] Na versão original: "*Electronic evidence: data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or*

oferece-nos uma definição que assenta no seguinte: "informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"[159]. Por sua vez, SILVA RODRIGUES procede a uma fusão entre conceitos e opta pela prova eletrónico-digital sendo esta "qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital"[160]. Esta aglutinação revela-se, aos nossos olhos, incorreta pois o conceito de prova eletrónica já tem em si o conceito de prova digital, porém não se reduz apenas a isto[161]. Se não vejamos. Como observa RAMALHO a prova eletrónica abrange não só "a prova em formato digital, mas também a prova em formato analógico, como sejam as gravações em fita vídeo e áudio ou fotografias em rolo fotográfico, os quais, apesar de *digitalizáveis*, não têm a sua origem em formato digital"[162].

Expectável será a circunstância da prova digital exigir cuidados especiais "pois um mero descuido pode torná-la irremediavelmente inutilizada"[163]. Ora, a prova digital pode estar presente em computadores, *tablets*, *smartphones* ou mesmo dispositivos de armazenamento USB, câmaras fotográficas ou de vídeo, aparelhos periféricos (*v.g.* impressoras), gravadores de áudio, sistemas de videovigilância, consolas de videojogos, entre outros[164]. Assim, dada esta pluralidade de fontes, na recolha de prova, conforme denota SÓNIA FIDALGO, pode ter-se acesso 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"[165]. Tendo em conta esta circunstância, os meios de obtenção de prova terão que ser adaptados a esta realidade, não podendo ser aceite o paralelismo que

---

computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence." STEPHEN MASON E BURKHARD SCHAFER, *The characteristics of electronic evidence*, in Stephen Mason and Daniel Seng (eds.), Electronic Evidence (4th edn, University of London 2017), p.19

[159] ARMANDO DIAS RAMOS, *Prova digital em Processo Penal: O Correio*… ob.cit., p. 95.

[160] BENJAMIM SILVA RODRIGUES, *Direito Penal Parte Especial*, Tomo I, Direito Penal Informático-Digital, 2009, p. 722.

[161] Cf. notas de rodapé 163 e 164 onde o autor critica a "fusão" e confusão dos conceitos prova eletrónica e prova digital *in* DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 101

[162] *Ibid*. p.100

[163] ARMANDO DIAS RAMOS, *Prova digital em Processo Penal: O Correio*… ob.cit., p. 97

[164] Exemplos avançados por DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 102

[165] SÓNIA FIDALGO, "A utilização da inteligência artificial no âmbito da prova digital …", ob.cit., p. 133

muitas vezes se observa entre as buscas físicas e apreensões e a obtenção de prova digital[166]. Isto porque a prova digital encerra em si determinadas caraterísticas que fazem desta uma prova que exige conhecimento e interpretação técnica específica no processo de recolha e análise que a tornam "diferente, vulnerável e especial"[167]. Os aspetos que caraterizam esta prova são o seu caráter temporário, fungibilidade, volatilidade[168] e imaterialidade/invisibilidade[169]

No que concerne ao caráter temporário está relacionado com o facto de, com o decurso do tempo, a prova digital deixar de existir. Ou seja, é uma prova extremamente efémera condenada ao desaparecimento em pouco tempo. É essencial, portanto, a sua recolha no mais curto espaço de tempo sob pena de desaparecimento e frustração de toda a investigação.

É fungível e volátil. A primeira caraterística deve-se ao facto de os dados informáticos poderem ser facilmente substituídos o que dificulta bastante a investigação[170]. A sua volatilidade prende-se com o facto de poderem ser ocultados ou alterados dados ou mesmo o seu desaparecimento com a verificação de certos eventos (falta de bateria do sistema informático[171]) ou ainda ser gravada nova informação sobre informação antiga.

É imaterial ou invisível pois se abrirmos fisicamente um computador não vamos encontrar nada no seu interior[172]. Ou seja, a prova digital não é algo palpável, corpóreo, físico. Assim, requerem-se cuidados acrescidos e uma intervenção qualificada na sua recolha porque um pequeno descuido poderá comprometer a investigação.

Uma última nota a propósito da plurilocalização da prova digital. Esta pode encontrar-se em vários locais virtuais dentro do mesmo sistema informático e em diversos locais geográficos[173]. Esta dispersão pode conduzir a uma dificuldade acrescida para a sua recolha.

---

[166] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 102
[167] ARMANDO DIAS RAMOS, *Prova digital em Processo Penal: O Correio*… ob.cit., p. 97
[168] *Ibid*. p. 98
[169] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 104
[170] ARMANDO DIAS RAMOS, *Prova digital em Processo Penal: O Correio*… ob.cit., p. 98
[171] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 106
[172] *Ibid*., pp. 104-105
[173] *Ibid*., p. 108

1.1. Dificuldades práticas colocadas pelo "pântano normativo"[174] em que se encontra a prova digital

Como já referimos, em termos legislativos e no que à prova digital diz respeito, estamos perante um verdadeiro "emaranhado legislativo". O facto deste tema ser regulado por três diplomas faz com que seja difícil operar uma concordância prática entre os diplomas[175], afirmando CONDE CORREIA que "as peças do puzzle não se encaixam facilmente"[176]. A este propósito e analisando criticamente, o legislador, aquando da consagração da prova digital, não devia ter optado pela criação de legislação extravagante como a Lei n.º 32/2008 e a Lei n.º 109/2009. Afigurava-se, na nossa perspetiva, muito mais profícuo se esta matéria tivesse sido regulada apenas e exclusivamente no CPP. Dada a importância do tema devia ter sido outro o cuidado do legislador. Porém, caso não fosse o propósito do legislador regular esta matéria exclusivamente no CPP (pela recodificação que impunha) e recorrer apenas a legislação extravagante deveria, conforme denota CONDE CORREIA, ter procedido à sua revogação formal[177] no que à prova digital diz respeito. Assim, seguimos a linha de pensamento de MILITÃO que afirma que a prova digital deveria ter sido delineada com base na obtenção de prova do regime geral (CPP)[178] e regulada nesse mesmo diploma. Obviamente com adaptações lógicas ao ambiente particular do ciberespaço, mas uma atualização do nosso processo penal à era digital é a solução legal mais coerente, necessária, facilitadora e, sobretudo, uniformizadora dado que "sem uma boa lei, por melhores que sejam os nossos juristas, dificilmente haverá bom direito"[179].

---

[174] Palavras de CONDE CORREIA a propósito da regulação legislativa da prova digital in JOÃO CONDE CORREIA, *Prova digital: as leis…* ob.cit., p. 30

[175] "Atualmente existem três regimes diversos de aquisição processual de dados de base, de tráfego e de localização: o regime processual penal geral, previsto no Código de Processo Penal e dois regimes especiais, o da Lei 32/2008, de 17 de julho e o da Lei 109/2009, de 15 de setembro (Lei do Cibercrime), todos com requisitos diversos e com diversas estipulações e implicações relativamente às obrigações de conservação dos dados. A sua compatibilização prática depende de esforço interpretativo" CARLOS PINHO, *Os problemas interpretativos resultantes da Lei nº 32/2008*, de 17 de julho, Revista do MP, nº 129, Jan-Mar 2012, p. 79.

[176] JOÃO CONDE CORREIA, *Prova digital: as leis que temos…,* ob.cit., p. 30

[177] A própria jurisprudência tem entendido neste sentido. Cf. Ac. TRE de 6/1/2015, processo 6793/11.2TDLSB-A.E1 que entendeu "*As Leis nº 32/2008, de 17-07 e 109/2009, de 15-09 (Lei do Cibercrime) revogaram a extensão do regime das escutas telefónicas, previsto nos artigos 187º a 190º do Código de Processo Penal, às áreas das "telecomunicações eletrónicas", "crimes informáticos" e "recolha de prova eletrónica*" disponível em: www.dgsi.pt

[178] RENATO LOPES MILITÃO, *A propósito da prova digital no processo penal*, ROA, Ano 72, jan/mar (2012), p. 266

[179] JOÃO CONDE CORREIA, *Prova digital: as leis que temos…,* ob.cit., p. 53

2. A recolha de prova digital no decurso da Ação Encoberta

Na realização da AE pode o agente que a está a realizar constatar que o suspeito armazena do seu dispositivo informático conteúdo ilícito essencial para a prossecução do processo. Pensemos no caso, por exemplo, de, no decurso da AE, o agente travar contacto com um suspeito que se dedica à disponibilização de imagens e vídeos com conteúdo ilícito sendo que, nesse contacto, o agente apercebe-se que este conteúdo se encontra localizado no computador pessoal desse suspeito. Será de todo o interesse para a investigação neste caso (e em outros semelhantes) ter acesso ao conteúdo presente nos dispositivos eletrónicos do suspeito sejam eles computador, *tablet*, telemóvel, *pens*, cartões de memória, etc, pois só assim se consegue sustentar de forma probatória o processo. Iremos nas próximas linhas analisar a possibilidade de recorrer à busca *online* como um eventual meio idóneo de obter essa mesma prova.

2.1. As buscas *online* como meio de obtenção de prova: uma possibilidade no nosso ordenamento?

Iniciando por um adiantamento de resposta à questão que inicia o presente ponto, as buscas *online* não são um meio de obtenção de prova admitido em Portugal não se encontrando regulado na legislação nacional[180]. Sendo este oculto, exige-se que, por força da reserva de lei[181], se encontre expressamente previsto na lei. Não existindo uma norma que preveja expressamente esta possibilidade[182], então esta não é admissível na investigação. Contudo, como infra concretizaremos, consideramos que este mecanismo se afigura de enorme importância para a investigação devendo este ser utilizado.

[180] Existe doutrina que entende que este método está consagrado no n.º 5 do art. 15º da LC. Não concordamos com esta perspetiva pois entendemos que o estabelecido é uma extensão da pesquisa prevista no n. º1 do qual, necessariamente, o visado tem conhecimento. Cf. SÓNIA FIDALGO, "A utilização da inteligência artificial no âmbito da prova digital…", ob.cit., p. 153

[181] Relativamente aos "procedimentos ocultos de investigação" COSTA ANDRADE refere que estes apenas são admissíveis, por força da reserva de lei, nos casos em que a lei autorize e legitime essas medidas. Acrescenta o autor que, com o advento tecnológico, esta afigura-se uma exigência de "importância e relevo crescente" sendo que toda a produção de prova que seja feita sem a existência de uma "nova e pertinente lei de autorização" será ilegal e ilegítima. Cf. MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob.cit., p. 112

[182] DAVID SILVA RAMALHO, *Métodos Ocultos*…, ob.cit., p. 222

Comecemos pelo que se entende por busca *online*. Segundo CONDE CORREIA a busca *online* permite através do uso de "várias técnicas informáticas à distância, via internet, aceder aos dados contidos num computador, observá-los, monitorizá-los, copiá-los sem o conhecimento ou consentimento do visado" permitindo-se ao "Estado […] intrometer-se num computador alheio e verificar o que lá está" [183]. Por sua vez, COSTA ANDRADE, entende a busca *online* como "conceito compreensivo e abrangente […] a que se reconduz um conjunto de intromissões nos sistemas informáticos, feitas através da *internet* e que se atualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas informáticos"[184]. Definido o conceito, importa sublinhar que as buscas *online* são distintas da pesquisa de dados informáticos previsto no art. 15.º da LC em que se estabelece o seguinte: "Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência". Assim, a nota diferenciadora reside no facto de a busca *online* ser um meio oculto do qual o suspeito não tem conhecimento que está a ser realizado (o suspeito não sabe que o seu computador se encontra ser vigiado e, eventualmente, dados a ser copiados), enquanto na pesquisa de dados existe conhecimento desta ação por força da entrega ao suspeito do despacho que autoriza aquela diligência e, conexo a isto, existe uma deslocação física até ao computador desse mesmo suspeito, os OPC dirigem-se fisicamente ao sítio em que esse computador se encontra (não pode ser feita à distância, através de "outro terminal informático"[185] *v.g.* nas instalações do OPC competente). Ainda a este propósito DIAS RAMOS discorda com a terminologia as buscas *online,* afirmando que estamos sim perante uma " «pesquisa de dados *online*», que é no fundo […] uma intervenção encoberta em sistemas informáticos"[186]. Já RITA CASTANHEIRA NEVES levanta uma outra questão afirmando que "a referência à presença da autoridade judiciária na diligência de pesquisa de dados informáticos no n.º 1 do art. 15.º, bem como o elenco das apreensões os dados informáticos nas alíneas a) a d) do n.º 7 do

[183]JOÃO CONDE CORREIA, *Prova digital: as leis que temos…,* ob.cit., p. 42
[184] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob.cit., p. 166
[185] RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações Eletrónicas Em Processo Penal*. Natureza e Respetivo Regime Jurídico do Correio Eletrónico enquanto Meio de Obtenção de Prova, 2011, p. 195
[186] ARMANDO DIAS RAMOS, *Prova digital em Processo Penal: O Correio*… ob.cit., p. 90

artigo 16.º da LC, deixam de fora a possibilidade de as instâncias formais de controlo poderem levar a cabo buscas sem que o visado seja diretamente confrontado com a diligência"[187]. E aqui concordamos inteiramente com CONDE CORREIA quando este quando este afirma "[…] nenhum desses dois argumentos é decisivo. A presidência do magistrado tanto pode ser para *in locu* a dirigir a diligência como para o fazer *online*. Ele não tem que estar no local onde está o computador, mas no local em que se acede."[188]

Importa agora atentar o que entendemos serem os benefícios da consagração desta medida e o que traz para a investigação criminal. A mais óbvia será o contributo para a descoberta da verdade material e para a recolha de provas. Conseguir ter acesso a todo o conteúdo do computador do suspeito pode ser a peça chave para que a investigação prossiga. A segunda prende-se com a própria informatização/digitalização da fenomenologia criminal. O mundo digital está presente no dia a dia de todos nós e, tal como já temos vindo a afirmar ao longo do nosso estudo, não trouxe consigo apenas benefícios. Assim, através de um computador uma pessoa pode planear ao pormenor a sua atividade criminosa podendo trazer, através da *internet*, novos elementos para a sua rede criminosa construindo-se assim uma grande teia que opera tanto fisicamente como digitalmente. Perante este lado obscuro da informática, o Direito tem que ser atual e ter uma resposta adequada ao "agora". Dado isto, as buscas *online* afiguram-se uma solução importante para a prevenção e repressão da criminalidade grave praticada digitalmente. Do outro lado da barricada temos a questão constitucional e os problemas que podem advir da utilização desta medida. São muitos os obstáculos levantados afirmando, autores como COSTA ANDRADE, que este mecanismo pode levar a uma "qualificada e drástica danosidade, do ponto de vista dos direitos fundamentais atingidos"[189]. Contudo, voltamos aqui a frisar que a conciliação com os DF's e eventual consagração processual desta medida se afigura exequível. Neste sentido, parece-nos bastante assertiva a decisão do Tribunal Federal Alemão que prevê a constitucionalidade do recurso a buscas *online* desde que sejam verificados "fortes e extremamente exigentes critérios de *proporcionalidade*"[190] tendo que se verificar um "perigo concreto […] para bens

[187] RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações Eletrónicas…,* ob.cit., p. 284
[188] JOAO CONDE CORREIA, *Prova digital: as leis que temos*…, ob.cit., nota de rodapé 29, p. 42
[189] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob.cit., p.166
[190] *Ibid.*, p. 168

jurídicos de importância transcendente para o individuo[191] ou para a comunidade organizada em Estado de Direito"[192].

Esta decisão do Tribunal Federal Alemão de 27/2/2008[193] afigura-se relevante por ter também inserido um novo direito constitucional: o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informations-technischer Systeme*). No que concerne a este ponto, estávamos perante um caso que contendia com o artigo § 5.2 (11) da Lei de Proteção da Constituição da Renânia do Norte-Vestefália[194] que permitia o acesso secreto a sistemas informáticos (busca *online*) quando existissem suspeitas da prática de crimes.[195] Como nota RAMALHO, o Tribunal Alemão esforçou-se para proceder ao enquadramento deste meio de obtenção de prova analisando-o inclusive à luz do direito à inviolabilidade do domicílio[196]. Porém, chegou à conclusão que existia uma "geral lacuna de proteção" afirmando que era necessário reconhecer um "novo direito fundamental emergente […] que tutele adequadamente a vida privada dos indivíduos contra acessos do Estado na área das tecnologias da informação, em particular quando, desse modo, o Estado tenha acesso a sistemas informáticos como um todo e não apenas a dados específicos de comunicação ou dados armazenados, a saber: o direito à integridade e confidencialidade dos sistemas informáticos […]."[197] Pretende-se, com a consagração deste novo direito fundamental, a proteção dos sistemas informáticos quando, no decurso investigação, possa existir acesso a dados pessoais do visado pela diligência de tal forma que, quem realiza a

---

[191] Como sejam a vida, o corpo ou a liberdade. Cf. JOÃO CONDE CORREIA, *Prova digital: as leis que temos…,* ob.cit., p.44

[192] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob.cit., p.169

[193] Versão oficial em inglês do acórdão disponível em: Bundesverfassungsgericht - Decisions - Provisions in the North-Rhine Westphalia Constitution Protection Act on online searches and on the surveillance of the Internet null and void consultado em 10/8/2021

[194] *"§ 5 Powers (2) In accordance with § 7, the constitution protection authority may apply the following measures to acquire information as intelligence service means: 11. secret monitoring and other reconnaissance of the Internet, such as in particular concealed participation in its communication facilities and searching therefor, as well as secret access to information technology systems also involving the deployment of technical means. Insofar as such measures constitute an encroachment on the secrecy of correspondence, post and telecommunication or are equivalent to such encroachment in terms of their nature and grievousness, the latter shall be permissible only under the preconditions of the Act re Article 10 of the Basic Law*" retirado da versão em inglês do acórdão

[195] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob. cit., p. 243; FABIANO MENKE, A *proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no Direito Alemão*, RJLB, Ano 5 (2019), nº 1, pp. 782 e 794.

[196] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., pp. 244-246.

[197] *Ibid.*, p. 247

investigação, possa ter uma "fotografia" da sua personalidade[198] (saber os seus gostos pessoais, o que faz no seu dia a dia, ter acesso a fotografias familiares,...). Neste âmbito de proteção estão também todos os sistemas que possam ser acedidos através do primeiro sistema informático alvo da investigação (por exemplo *webmails*)[199]. Em suma, pretende-se salvaguardar a potencial obtenção de informações sensíveis do suspeito no decorrer do acesso a um sistema informático[200].

Afigura-se pertinente a análise desta decisão pois consideramos que se revela de extrema utilidade a consagração de um direito fundamental que tutele o ambiente virtual. Como assinala RAMALHO, que acompanhamos totalmente, também no OJ português podia ser adotada uma solução semelhante dando-se a importância devida ao tema considerando-se, assim, o direito à não intromissão no ambiente digital ou à confidencialidade e integridade dos sistemas informáticos como uma decorrência do princípio do Estado Democrático e do direito ao livre desenvolvimento da personalidade, da reserva da intimidade da vida privada, ao sigilo da correspondência e dos outros meios de comunicação privada e à utilização da informática em particular a proibição de acesso a dados de terceiros[201]. Consideramos, portanto, que uma solução nos moldes da jurisprudência alemã daria uma resposta muito mais completa e uniforme dada a emergência tecnológica que se tem verificado (e que continuará). Tal passo terá que ser dado.

Acompanhamos CONDE CORREIA quando este afirma que "o sistema processual penal tem que estar preparado para resolver os graves problemas que lhe venham a ser colocados"[202] e só através de mecanismos como este é que o processo penal estará preparado para combater a criminalidade extrema. Assim, no nosso entender, é necessária a consagração deste meio de obtenção de prova. Contudo, teríamos que estabelecer critérios apertados para recorrer a esta medida em linha com o que foi estabelecido pelo Tribunal Federal Alemão (a existência de um perigo concreto, perigo esse que ameaça bens jurídicos

---

[198] FABIANO MENKE, A *proteção de dados e o direito*… ob.cit., p.800
[199] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 248
[200] "Firstly, it protects the interest of a user of an information technology system in ensuring that the data created, processed and stored by the system remains confidential. Secondly, this right is violated if the integrity of such a system is affected by the system being accessed in such a way that third parties can use its performance, functions and storage contents" WIEBKE ABEL AND BURKHARD SCHAFER, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG*, NJW 2008, 822, Scripted, Volume 6, Issue 1, April 2009, p. 120; DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 248
[201] *Ibid*. 251
[202] JOÃO CONDE CORREIA, *Prova digital: as leis que temos…,* ob.cit., p. 44

fundamentais como a vida, corpo e liberdade). Outro ponto que consideramos essencial é permitir a medida para um catálogo restrito de crimes que lesem, de facto, os DF's já referidos. Sejam eles crimes de terrorismo, criminalidade organizada ou pornografia infantil. Assim, na sua consagração deverá o legislador definir dois aspetos essenciais para esta medida: o quando e como. Ou seja, em que situações se justifica o uso de buscas *online* e que moldes essa atuação deverá seguir. Por último, consideramos que tal medida, dependendo da fase processual, terá que ser previamente autorizada sempre por um Juiz ou JIC. Não podemos ignorar que as buscas *online* seriam um enorme contributo para a investigação criminal que tanto é dificultada em ambiente digital dada a astúcia crescente dos criminosos, seria uma forma de os agentes que investigam não ficarem para trás ou correrem atrás do prejuízo, podendo prevenir a prática de inúmeros ilícitos que, a acontecer, poderão ter efeitos muito nefastos para todos nós enquanto comunidade.

2.2. Conciliação da busca *online* com os Direitos Fundamentais-breve análise

Tendo em mente estas exigências acima sublinhas na previsão das buscas *online*, analisaremos agora a questão sob o ponto de vista constitucional. Tentaremos perceber que DF's poderão ser lesados com a consagração das buscas *online* e o que se deverá ter em conta num eventual desenho legislativo futuro.

As buscas *online*, como acima referido, traduzem-se num meio oculto de obtenção de prova que pertence à categoria dos métodos ocultos de investigação[203]. Conforme nos ensina COSTA ANDRADE os métodos ocultos "representam uma intromissão nos processos de acção, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam"[204]. Por isso mesmo, num plano material substantivo[205], e em abstrato, um método oculto pode lesar DF's como: *o direito à reserva da intimidade da vida privada, o direito à inviolabilidade do domicílio, o direito à imagem e à palavra e o direito à confidencialidade e integridade dos sistemas informáticos*.

[203] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado*"*, ob.cit., p. 104
[204] *Ibid.* p. 105.
[205] *Ibid*., p. 106

Afigura-se, portanto, difícil a "compatibilização"[206] entre um método oculto de obtenção de prova e os DF's.

Nas próximas linhas analisaremos sumariamente o conteúdo dos dois primeiros[207] e em que medida podem ser lesados pela busca *online.*

A) DIREITO À RESERVA DA INTIMIDADE PRIVADA

O direito à reserva da intimidade privada tem tutela internacional e, também, no próprio OJ português. Começando pela proteção internacional, vem este direito consagrado no art. 12.º da Declaração Universal dos Direitos do Homem, no art. 8.º da Convenção Europeia dos Direitos do Homem, bem como no art. 17.º do Pacto Internacional de Direitos Políticos e Civis. Ao nível nacional, temos este direito previsto no art. 26.º da Lei Fundamental e também no art. 80.º do CC.

Para melhor entendimento do conceito de reserva da intimidade privada recorremos à jurisprudência constitucional. O TC já se debruçou sobre este tema em inúmeras ocasiões sendo que, no seu Ac. nº 306/2003 de 25 de junho de 2003, processo n.º 382/2003[208], define o direito à reserva da intimidade da vida privada como "direito a uma esfera própria inviolável, onde ninguém deve poder penetrar sem autorização do respetivo titular, ou, noutra formulação, como o direito que toda a pessoa tem a que permaneçam desconhecidos determinados aspetos da sua vida, assim como a controlar o conhecimento que terceiros tenham dela" acrescentando, ainda, o seguinte: "este direito analisa-se principalmente em dois direitos menores: o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem […]". Ou seja, este direito carateriza-se, essencialmente, por conferir ao individuo uma área inviolável da sua vida privada à qual os demais não terão acesso.

Definir o conceito de "vida privada" revela-se uma missão de difícil execução pois como denota MOTA PINTO é uma noção "obscura e sem um verdadeiro conteúdo

[206] SÓNIA FIDALGO, "A utilização da inteligência artificial no âmbito da prova digital…", ob.cit., p. 131.
[207] Apesar de se afigurar relevante, não se levará a cabo um estudo aprofundado de cada um dos DF's mencionados. Para estudo aprofundado sobre a análise dos DF's à luz dos métodos ocultos de investigação Cf. MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob.cit., pp. 148-155
[208] Disponível em: www.tribunalconstitucional.pt

preciso"[209]. Assim, conforme acrescenta RICARDO LEITE PINTO este é um direito "pluridimensional e complexo"[210] dado que pode ser restringido através das mais diversas formas avançando o autor com algumas situações como a "publicação de imagens, pelas escutas telefónicas, pela devassa de dados informáticos, pela invasão do domicílio, etc."[211]

Atualmente entender este conceito revela-se uma tarefa de especial complexidade pois com o advento tecnológico e o uso massivo de redes sociais torna-se complicado delinear fronteiras entre aquilo que é público e aquilo que é privado. Assim, factos que hoje são encarados como públicos podem ter sido anteriormente vistos como privados e vice-versa[212].

Ao analisarmos as buscas *online* à luz do direito à intimidade da vida privada concluímos que este direito pode ser bastante restringido. Vejamos porquê. No decurso desta diligência pode ter-se acesso a dados de índole pessoal do suspeito como os seus gostos, rotina diária, situação económica, financeira, dados sobre a sua saúde e muitos outros. O computador é visto, atualmente, como um repositório onde tudo o que é relevante para a nossa vida é lá armazenado[213]. Assim, ao realizar-se a busca *online*, ao vasculhar-se o conteúdo presente no computador, o agente pode ter acesso a todos estes dados da "esfera íntima da intimidade"[214] do investigado que corresponde à "área nuclear, inviolável e intangível da vida privada, protegida contra qualquer intromissão das autoridades ou particulares"[215]. Podemos, portanto, assistir a uma restrição a este direito com esta diligência.

B) DIREITO À INVIOLABILIDADE DO DOMICÍLIO

Este direito encontra-se consagrado no art. 34.º da CRP.

---

[209] PAULO MOTA PINTO, *A protecção da vida privada na jurisprudência do Tribunal Constitucional*, 2006, p. 7. Disponível em: https://www.tribunalconstitucional.es/es/trilateral/documentosreuniones/30/ponencia%20portugal%202006.pdf consultado em 25/08/2021

[210] RICARDO LEITE PINTO, *Liberdade de Imprensa e Vida Privada,* ROA, Ano 54- 1994, p. 62

[211] *Ibid*

[212] JOÃO CONDE CORREIA, *Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?*- Revista do MP, nº 79, Julho/Setembro de Ano 20, 1999, p. 47

[213] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado*",* ob.cit., p. 167

[214] Esta esfera insere-se na Teoria dos Três Graus (esfera da intimidade, esfera da vida privada e esfera da vida normal da relação) criada pelo Tribunal Constitucional Federal em 1973. Cf: MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova*… ob.cit., p.94

[215] *Ibid.*

Tradicionalmente entende-se que com a consagração constitucional deste direito se pretende proteger a entrada "física e corpórea por parte de pessoas indesejadas"[216] no domicílio que pode ser entendido como o local em que se praticam "atos relacionados com a vida familiar e com a esfera íntima privada"[217]. Também nesta linha já se pronunciou o TC a propósito do conceito de domicílio entendendo-o como sendo um "espaço fechado e vedado a estranhos, onde, recatada e livremente, se desenvolve toda uma série de condutas e procedimentos característicos da vida privada e familiar"[218].

Contudo, neste estudo, a pertinência desta questão não se prende com uma entrada física no domicílio do investigado porque, ao contrário das buscas tradicionais, tal não ocorre. Estamos sim a analisar sob o ponto de vista digital. Noutras palavras, será que o agente que leva a cabo uma busca *online*, sem que o suspeito tenha conhecimento disso, pode lesar o direito à inviolabilidade do domicílio? Consideramos que não e vejamos porquê.

Em primeiro lugar, atendendo a todos os progressos tecnológicos e científicos que se vão observando, como já temos vindo a frisar em diversas questões, o próprio conceito de domicílio também sofre mutações tendo que se atualizar ao "mundo atual". Assim, neste sentido, afirmam GOMES CANOTILHO e VITAL MOREIRA que não podemos considerar que este direito se encontra lesado apenas quando existe uma introdução física no domicílio tendo que se atender aos "modernos meios técnicos [que] possibilitam a invasão do domicílio mediante meios eletrónicos (…)"[219]. Também tendo em conta esta mudança de paradigma o Tribunal Federal Alemão pronunciou-se afirmando que este direito estava "primacialmente votado à defesa do titular do domicílio contra a indesejada presença física […]. Desde então surgiram novas possibilidades de colocação do direito fundamental em perigo. Os atuais dados tecnológicos permitem a intromissão na esfera espacial de outras formas. O fim da proteção da norma do direito fundamental resultaria frustrado se a proteção contra uma devassa da habitação com recurso a meios técnicos não fosse abrangida […]".[220] Revela-se necessário alargar o leque de possibilidades que poderão comprometer o núcleo

[216] MANUEL DA COSTA ANDRADE, "Bruscamente no Verão passado", ob. cit., p. 151
[217] JORGE MIRANDA E RUI MEDEIROS, *Constituição da República Portuguesa Anotada*, tomo I, 2010, p. 759
[218] Ac. TC n.º 452/89 de 28 de junho de 1989, processo n.º 15/87 disponível em: www.tribunalconstitucional.pt

[219] J.J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*- Artigos 1º a 107º, 4.º Ed. Revista, 2007, pp. 540-541
[220] MANUEL DA COSTA ANDRADE, "Bruscamente no verão passado", ob.cit., pp. 151-152

de proteção deste direito como por exemplo a introdução no domicílio de dispositivos de escutas, de transmissão de imagens ou sons e meios de captação à distância[221].

Mas neste alargamento de cenários onde enquadramos as buscas *online*? Ora, como sabemos, o agente não se encontra fisicamente inserido no domicílio do suspeito, contudo, como assinala COSTA ANDRADE, acede de forma oculta, por via internet, aos dados contidos no computador desse sujeito que pode acontecer de forma instantânea e descontínua ("*espelho*") ou de forma contínua ("*monitoring*")[222]. A este propósito podemos levantar uma questão: se esse computador que está a ser acedido se encontra no domicílio do suspeito assistimos a uma compressão do direito da inviolabilidade do domicílio? Consideramos que não. Primeiro porque nos parece uma posição demasiado extremada e, em segundo lugar, a localização do computador acaba por ser indiferente dado ser algo completamente aleatório que não depende dos agentes que realizam a busca. Esta tanto pode ser iniciada quando o suspeito se encontra num café a usar esse computador, ou pode ser iniciada quando este se encontra em casa. Ter em conta um aspeto tão fortuito acaba por se revelar inútil.

Por tudo o que vem sendo exposto, concluímos que os progressos tecnológicos ocorridos contribuíram para uma mudança no conceito de domicílio sendo que, atualmente, este não abrange apenas o domicílio físico. Como tal, temos assistido a novas formas de compressão deste direito à inviolabilidade do domicílio que trazem consigo novas questões. Porém, como analisámos, não consideramos que este direito possa ser ferido com a utilização de uma busca *online.*

2.2.1. Balanço Final

Analisado o conteúdo e potenciais restrições que os DF's estudados podem sofrer, afigura-se relevante fazer um balanço.

De facto, é inegável que a utilização de buscas *online* pode colidir com a proteção conferida pelos DF's. Estamos perante um "terreno movediço"[223] pois se, por um lado, cabe

[221] *Ibid*., p. 152
[222] *Ibid.* p. 153
[223] ISABEL ONETO, *O agente infiltrado*…, ob.cit., p. 158

ao Estado e se afigura essencial proteger os DF's dos cidadãos também de igual importância é a segurança, o direito à vida, à liberdade e muitos outros direitos constitucionalmente previstos.

Ora, a tensão entre pólos como o direito à reserva da intimidade privada e o direito à segurança pode ocorrer nesta temática. Porém, como consagra o n. º2 art. 18.º da CRP, os DF's podem, em determinadas ocasiões, ser restringidos na medida do "necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos". Temos aqui subjacente uma ideia de proporcionalidade, ou seja, temos que fazer uma análise casuística de forma a perceber se aquele direito fundamental que se pretende proteger é superior ao que irá ser sacrificado. Cabe, portanto, legislador desenhar os moldes em que a medida será admissível[224], o que, para nós, se afigura um passo urgente e de extrema importância para o combate à criminalidade grave e organizada.

Assim, perante este surgimento de nova criminalidade são necessários novos meios de resposta sobretudo porque cabe ao Estado (*in casu* à Polícia), segundo o art. 272.º/1 da CRP, defender os direitos dos cidadãos. Se os meios ao dispor não se afiguram suficientes terão que se encontrar outros mecanismos, não podemos é aceitar a existência de lacunas que conduzem a impunidades. Há que ter sempre em mente que os DF's não são ilimitados, absolutos e alguns terão que "cair" para que outros sejam protegidos[225]. É neste fio da navalha que operarão as buscas *online.* A conciliação entre a medida e os DF's é possível, basta que o legislador tenha "imaginação legislativa"[226].

[224] DAVID SILVA RAMALHO, *Métodos Ocultos*… ob.cit., p. 227
[225] "Os direitos fundamentais, enquanto princípios que são, não se revestem de carácter absoluto, antes são limitados internamente, para assegurar os mesmos direitos a todas as outras pessoas, e também externamente, para assegurar outros direitos fundamentais ou interesses legalmente protegidos que com eles colidam, mediante a harmonização entre uns e outros, a qual sempre implicará o sacrifício, total ou parcial, de um ou mais valores" Ac. STJ de 29/11/2016, processo n.º 7613/09.3TBCSC.L1.S1. Disponível em www.dgsi.pt
[226] JOÃO CONDE CORREIA, *Prova digital: as leis que temos…,* ob.cit., p. 59

CONCLUSÕES

I. Desde sempre o Direito Processual Penal é desafiado com novos problemas às quais tem que dar resposta. Assim, para novos crimes exigem-se novos métodos. Neste seguimento, é criado no nosso OJ pela primeira vez, com o DL n.º 430/83 de 13 de dezembro (Lei da Droga), uma figura importantíssima para dar resposta a determinada criminalidade: o AE. Esta figura revela-se de excecional importância tendo, atualmente, o seu diploma próprio- o RJAE (Lei n.º 101/2001). Contudo, para se recorrer a esta figura terão que ser cumpridos requisitos apertados o que faz desta uma solução excecional.

II. Mas, os tempos vão mudando e novos problemas vão surgindo sendo necessário um acompanhamento por parte do Processo Penal. Numa sociedade modernizada e tecnológica na qual hoje nos inserimos, os sistemas informáticos assumem um papel primordial na nossa rotina. Se, por um lado, a internet aproxima o mundo e facilita a nossa vida em variados campos; por outro, com a sua massiva utilização a probabilidade de esta ser usada para o cometimento de ilícitos é elevada.

III. Tendo isto em vista, a CCiber do Conselho da Europa de 23 de novembro de 2001 foi o primeiro diploma internacional que versou sobre a cibercriminalidade pretendendo-se essencialmente a harmonização das várias legislações no combate à cibercriminalidade.

IV. A nível nacional, foi a LC que transpôs para a OJ portuguesa a Decisão Quadro n.º 2005/222/JAI, de 24 de fevereiro, relativa a ataques contra sistemas de informação adaptando o nosso direito interno à CCiber. A LC foi antecedida pela LCI (Lei n.º 109/91, de 17 de agosto).

V. Neste diploma, previa-se, no seu art. 19.º, a possibilidade de recurso a AE no âmbito do combate à cibercriminalidade. Porém, remete-se a aplicação destas para o regime geral concebido para o mundo físico.

VI. As dificuldades que o ambiente digital convoca são das mais variadas índoles e complexidade não sendo suficiente aplicar um regime que não é, de todo, pensado para responder a questões particulares como as que são colocadas pelo ambiente digital.

VII. Estas Ações afiguram-se de extrema utilidade para a investigação criminal e consideramos que deve existir uma intervenção legislativa que olhe para estas ações "por si só" e deixe de as colar a realidades distintas como se de uma única coisa se tratasse.

VIII. No decurso da AE não podem ser esquecidos os mais importantes e elementares princípios do processo penal sendo que tal ação terá que ter sempre em conta os limites à descoberta da verdade material em particular as proibições de prova.

IX. Para adensar as dificuldades sentidas, delimitar as fronteiras entre infiltração e provocação em ambiente digital revela-se uma tarefa bastante árdua. Principalmente porque no plano prático o ciberespaço traz consigo problemas e questões particulares. Devia o legislador, aquando da criação da LC e admissibilidade do uso do AE digital, ter densificado o seu conceito, requisitos, limites, meios e modos de atuação, criando normas que se adaptassem ao mundo digital.

X. No que à recolha de prova diz respeito, consideramos que se afigura de enorme utilidade a eventual previsão das buscas *online*. Apesar da sua potencial lesão para os DF's tal medida afigura-se verdadeiramente essencial para o sucesso da investigação criminal digital.

XI. Exige-se, portanto, uma intervenção legislativa que autonomize as AE Digitais equacionando-se sempre os problemas particulares que esta realidade convoca e abandonando-se a resposta atual que remete para um regime que deixa diversas zonas cinzentas. Não se entende a solução do legislador pois acaba por tornar inútil uma figura que pode ter um papel verdadeiramente essencial no combate à cibercriminalidade. Outro ponto a não esquecer pelo legislador será a consagração das buscas *online* que constituirá um dos meios de obtenção de prova mais importantes do nosso OJ. Obviamente que dada a sua danosidade tal terá que ser construído com base em critérios apertados e ser admitida pontualmente. Porém, ainda existe flexibilidade constitucional para que tal suceda, basta que o legislador se proponha a tal.

XII. Assim, afigura-se imperativo que o legislador observe todo o desenvolvimento tecnológico que se vem verificando e perceba que o Processo Penal

ficou inerte e incapaz de responder a determinados problemas. Não é isto que se espera de um Processo Penal que se pretende eficaz. Resta-nos, portanto, aguardar que tal ocorra.

BIBLIOGRAFIA

— ANTÓNIO HENRIQUES GASPAR, "As ações encobertas e o processo penal: questões sobre a prova e o processo equitativo" in: *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, 2004

— ARMANDO DIAS RAMOS, Prova digital em Processo Penal: O Correio Eletrónico, Chiado Editora, 2017

— BENJAMIM SILVA RODRIGUES, *Direito Penal Parte Especial*, Tomo I, Direito Penal Informático-Digital, Coimbra Editora, 2009

— CARLOS PINHO, *Os problemas interpretativos resultantes da Lei nº 32/2008*, de 17 de julho, Revista do MP, nº 129, Jan-Mar 2012

— CAROLINA PEREIRA, *O Entendimento Jurisprudencial do Tribunal Europeu dos Direitos do Homem (TEDH) acerca da atuação do Agente Infiltrado* in: RIDB, Ano 1 (2012), nº 11

— DANIEL BENTO ALVES, "Uso de Malware em investigação criminal" in *Actualidad Jurídica Uría Menéndez*, nº47, 2017

— DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017

— "Investigação criminal na Dark Web" in *Revista da Concorrência e Regulação*, nº 14/15, abril-setembro 2013

— Dicionário da Língua Portuguesa Contemporânea da Academia das Ciências de Lisboa, II Vol., 2001

— Dicionário Jurídico, *Vol II Direito Penal e Direito Processual Penal*, 2009

— DUARTE RODRIGUES NUNES, O*s meios de obtenção de prova previstos na Lei do Cibercrime*, Coimbra: Gestlegal, 2018

— Enciclopédia Fundamental Verbo, Editor: Verbo, 1989

— FABIANO MENKE, A *proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no Direito Alemão*, RJLB, Ano 5 (2019), nº 1

— FEDERICO BUENO DE MATA, *El Agente Encubierto en Internet: Mentiras Virtuales para alcanzar la Justicia*, 2012

— GERMANO MARQUES DA SILVA, *Bufos, Infiltrados, Provocadores e arrependidos, Os princípios democrático e da lealdade em processo penal*, Direito e Justiça, Revista da Faculdade de Direito da Universidade Católica, Vol. VIII, Tomo 2, 1994

— *Meios processuais expeditos no combate ao crime organizado (A Democracia em perigo?)* in Lusíada.Direito, Revista de Direito da Universidade Lusíada, n.º3, 2005

— ISABEL ONETO, *O agente infiltrado- Contributo para a compreensão do regime jurídico das ações encobertas*, Coimbra Editora, 2005

— J.J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*- Artigos 1º a 107º, 4.º Ed. Revista, 2007

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

— JOÃO CONDE CORREIA, Contributo para a análise da inexistência e das nulidades processuais *in* Stvdia Ivridica, 44, Boletim da Faculdade de Direito, Coimbra, Coimbra Editora, 1999

— *Prova digital: as leis que temos e a lei que devíamos ter*, Revista do Ministério Público 139, Ano 35, julho/setembro 2014

— *Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?*- Revista do MP, nº 79, Julho/Setembro de Ano 20, 1999

— JORGE DE FIGUEIREDO DIAS, *Direito Penal- Parte Geral*, Coimbra: Gestlegal, 2019

— *Direito Processual Penal*, reimpressão da 1.ª Edição de 1974, 2004

— *Direito Processual Penal: Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por Maria João Antunes*, Coimbra: Secção de textos da Faculdade de Direito da Universidade de Coimbra 1998-1989

— JORGE MIRANDA E RUI MEDEIROS, Constituição da República Portuguesa Anotada, tomo I, Coimbra Editora, 2.ª edição, 2010

— KRISTIN FINKLEA, "Dark Web", *Congressional Research Service*, março 2017

— MANUEL AUGUSTO ALVES MEIREIS, "Homens de confiança"- Será o caminho? In *II Congresso de Processo Penal* (coord. : Manuel Monteiro Guedes Valente), 2006
— *O Regime das Provas Obtidas pelo Agente Provocador Em Processo Penal*, 1999

— MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão passado*", A reforma do Código de Processo Penal- Observações críticas de uma lei que podia e devia ter sido diferente, 2009
— "Métodos Ocultos de Investigação Criminal: plädoyer para uma teoria geral", in *Que futuro para o direito* processual penal? *Simpósio em homenagem a Jorge Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português (coord. Mário Ferreira Monte)*, 2009,
— *Sobre as proibições de prova em processo penal*, 1.º Edição (Reimpressão) Coimbra Editora, 2013
— MARIA JOÃO ANTUNES, *Direito Processual Penal*, 2017
— NUNO BRANDÃO, *O whistleblowing no ordenamento jurídico português*, Revista do MP 161: janeiro : março 2020
— PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, 2010
— PAULO MOTA PINTO, *A protecção da vida privada na jurisprudência do Tribunal Constitucional*, 2006
— PEDRO DIAS VENÂNCIO, *Lei do Cibercrime* Anotada e Comentada, 2011
— PEDRO SOARES DE ALBERGARIA/PEDRO MENDES LIMA, *O Crime de Detenção de Pseudopornografia Infantil — Evolução ou Involução?* In: Revista JULGAR - N.º 12 (especial) – 2010
— PEDRO VERDELHO, ROGÉRIO BRAVO, MANUEL LOPES ROCHA, *Leis do Cibercrime*- Vol. I.
— RENATO LOPES MILITÃO, *A propósito da prova digital no processo penal*, ROA, Ano 72, jan/mar (2012)
— RICARDO LEITE PINTO, *Liberdade de Imprensa e Vida Privada*, ROA, Ano 54-1994

— RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações Eletrónicas Em Processo Penal*. Natureza e Respetivo Regime Jurídico do Correio Eletrónico enquanto Meio de Obtenção de Prova, 2011
— RUI PEREIRA, «O "agente encoberto" na ordem jurídica portuguesa» in *Medidas de Combate à Criminalidade Económico-Financeira*, 2004
— SANDRA PEREIRA, "A recolha de prova pelo agente infiltrado", in *Prova Criminal e direito de defesa: estudos sobre a teoria da prova e garantias de defesa em processo penal*, 2017
— SÓNIA FIDALGO, "A utilização da inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo" In A Inteligência Artificial no Direito Penal (Coord. Anabela Miranda Rodrigues), Almedina, 2020
— STEPHEN MASON E BURKHARD SCHAFER, *The characteristics of electronic evidence*, in Stephen Mason and Daniel Seng (eds.), Electronic Evidence (4th edn, University of London 2017)
— STEPHEN MASON, *Internacional Electronic Evidence*, Londres: British Institute of Comparative Law, 2008
— SUSANA AIRES DE SOUSA, *Ações Encobertas (e outras figuras próximas) na investigação da criminalidade económico-financeira*, in revista JULGAR, n.º38, 2019
    — *Agent Provocateur e meios enganosos de prova. Algumas reflexões*., in Liber Discipulorum para Jorge de Figueiredo Dias, 2003
    — Neurociências e Processo Penal: Verdade Ex Machina? In *Estudos em Homenagem ao Prof. Doutor Manuel da Costa Andrade*, Volume II, 2017
— WIEBKE ABEL AND BURKHARD SCHAFER, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG*, NJW 2008, 822, Scripted, Volume 6, Issue 1, April 2009

JURISPRUDÊNCIA

Acórdãos do Tribunal Constitucional (consultados em: www.tribunalconstitucional.pt/tc/acordaos/ **)**

Ac. do TC nº 607/2003

Ac. do TC n.º 578/98

Ac. do TC nº 306/2003

Ac. do TC n.º 452/89

Acórdãos do Supremo Tribunal de Justiça (disponíveis em: www.dgsi.pt**)**

Ac. STJ de 29 de novembro de 2016

Ac. STJ de 20 de fevereiro de 2003

Ac. STJ de 13 de janeiro de 1999

Ac. STJ de 12 de março de 2008

Acórdãos do Tribunal da Relação de Lisboa (disponíveis em: www.dgsi.pt**)**

Ac. do TRL 20 de maio de 2010

Ac. do TRL de 22 de janeiro de 2013

Ac. do TRL de 23 de março de 2011

Ac. do TRL de 5 de maio de 2010

Acórdãos do Tribunal da Relação de Évora (disponíveis em: www.dgsi.pt**)**

Ac. do TRE 20 de janeiro 2015

Ac. do TRE de 6 de janeiro 2015

Acórdãos do Tribunal Europeu dos Direitos do Homem (disponível em: https://hudoc.echr.coe.int/ **)**

Ac. Teixeira de Castro contra Portugal, 9 de junho de 1998

Espanha

Tribunal Supremo (disponível em https://vlex.es/libraries/jurisprudencia-2)

Sentença Tribunal Supremo, Sala Segunda, de lo penal, n.º 767/2007, 3 de Octubre de 2007

Alemanha

BverfG (Disponível em: https://www.bundesverfassungsgericht.de/)

BVerfG, de 27 de fevereiro de 2008 – 1 BvR 370/07, 1 BvR 595/07

LINKS

- https://debates.parlamento.pt/catalogo/r3/dar/01/08/02/099/2001-06-21/16
- https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d
- https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention and protocol/ETS_185_Portugese-ExpRep.pdf
- https://www.cicdr.pt/documents/57891/128776/Conven%C3%A7%C3%A3o+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c
- https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_3_isp_eua.pdf
- https://sgp.fas.org/crs/misc/R44101.pdf

— https://www.publico.pt/2020/11/11/mundo/noticia/policia-desmantela-rede-mundial-pedofilia-centro-australia-1938741

— https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725

— https://www.irishtimes.com/news/technological-level-of-wonderland-network-shocked-all-investigators-1.189298

— https://www.publico.pt/2014/10/22/tecnologia/noticia/primeira-condenacao-no-caso-sweetie-a-crianca-virtual-abordada-por-predadores-sexuais-1673760

— https://www.tribunalconstitucional.es/es/trilateral/documentosreuniones/30/ponencia%20portugal%202006.pdf