Universidade do Minho
Escola de Direito

Ana Isabel Pereira Braga

Ações encobertas em ambiente digital – a emergência da criação de um regime jurídico autónomo

março de 2022

Ações encobertas em ambiente digital – a emergência da criação de um regime jurídico autónomo

Ana Isabel Pereira Braga

UMinho | 2022

Universidade do Minho
Escola de Direito

Ana Isabel Pereira Braga

Ações encobertas em ambiente digital – a emergência da criação de um regime jurídico autónomo

Dissertação de Mestrado
Mestrado em Direito Judiciário (Direitos Processuais e Organização Judiciária)

Trabalho efetuado sob a orientação do(a)
Professora Doutora Ana Raquel Oliveira Pereira Conceição

março de 2022

AGRADECIMENTOS

Uma vez terminado o presente estudo, é chegado o momento de deixar os mais sentidos agradecimentos a todos aqueles que contribuíram para que esta investigação pudesse ganhar vida:

À minha orientadora, a Sra. Professora Doutora Ana Raquel Conceição, por todos os preciosos ensinamentos e por estar sempre disponível para me ajudar.

À minha família e amigos, por me terem apoiado sempre.

Ao meu namorado, que sempre acreditou em mim, dando-me alento e motivação, por toda a paciência e horas perdidas de volta deste trabalho, por todos os valiosos conhecimentos partilhados. Por tudo.

A todos, o meu maior obrigada!

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

O aparecimento das novas tecnologias trouxe consigo um novo conceito de criminalidade e um novo *modus operandi* que a investigação criminal tem, imperativamente, de ter em linha de conta, para que possa realizar o seu propósito de uma forma mais eficaz. Deixamos de assistir, com tanta frequência, à dita criminalidade tradicional, onde a prática do crime sempre se situou no plano físico, para agora estar perante uma crescente deslocação do crime para o ambiente digital, para o aparecimento de crimes informáticos e para a utilização das referidas tecnologias para ludibriar os órgãos de polícia criminal. A criminalidade digital aumentou de forma exponencial, sendo necessário o recurso a métodos ocultos de investigação, como é o caso das ações encobertas.

Para a elaboração da presente dissertação tomamos por mote precisamente compreender como se realizam as ações encobertas no ambiente digital e qual o regime jurídico atualmente aplicável às mesmas.

Com esta análise, começamos por procurar compreender como se relacionam as ações encobertas em ambiente digital com as disposições normativas atinentes à prova presentes no Código de Processo Penal e em variados diplomas avulsos. A partir dessa relação, foi possível entender como é que as ações encobertas apareceram no ordenamento jurídico português, quais as normas a estas aplicáveis e como é que o aparecimento das novas tecnologias veio influenciar a prática de crimes e, consequentemente, o recurso a este meio de obtenção de prova.

Uma vez analisada toda a informação *supra* mencionada, identificamos quais as especificidades das ações encobertas em ambiente digital e averiguamos até que ponto as mesmas se encontram devidamente acauteladas com o regime jurídico atualmente vigente. Face ao conhecimento reunido, procuramos observar potenciais aspetos que o mesmo não considera e compreender qual o impacto desta desconsideração.

Concluímos que existe uma necessidade clara de um texto legal especificamente dedicado ao tratamento e regulamentação das ações encobertas em ambiente digital, que abarque todas as suas características. Explicitamos o porquê e, por fim, apresentamos um esboço do que entendemos que deve ser o regime jurídico aplicável às ações encobertas em ambiente digital.

Palavras-chave: Ações Encobertas – Ambiente Digital – Crimes Informáticos – Regime Jurídico Autónomo

ABSTRACT

The emergence of new technologies has brought with it a new concept of criminality and a new modus operandi that criminal investigation must imperatively take into account, so that it can carry out its purpose more effectively. We are no longer witnessing, so often, the so-called traditional crime, where the practice of crime has always been located on the physical world, to now be faced with a growing displacement of crime to the digital environment, the emergence of computer crimes and the use of mentioned technologies to deceive the criminal police entities. Digital crime has increased exponentially, requiring the use of hidden methods of investigation, such as undercover operations.

For the elaboration of this dissertation, we took as a motto precisely to understand how undercober operations are carried out in the digital environment and which legal regime currently applies to them.

With this analysis, we started by trying to understand how undercover operations in the digital environment are related to the normative provisions regarding evidence present in the Criminal Procedure Code and in various separate diplomas. From this relationship, it was possible to understand how undercover operations appeared in the Portuguese legal system, which rules apply to them and how the emergence of new technologies has influenced the practice of crimes and, consequently, the use of this mean of obtaining evidence.

Once all the information mentioned above has been analyzed, we identified the specifics of the undercover operations in the digital environment and found out to what extent they are properly safeguarded under the legal regime currently in force. In view of the knowledge gathered, we observed potential aspects that it does not consider and understood the impact of this disregard.

We concluded that there is a clear need for a legal text specifically dedicated to the treatment and regularization of undercover operations in the digital environment, covering all its characteristics. We explained why and, finally, we presented an outline of what we understand the legal regime applicable to undercover operations in the digital environment should be.

Keywords: Autonomous Legal Regime – Computer Crimes – Digital Environment – Undercover Operations

ÍNDICE

INTRODUÇÃO

Nos mais recentes anos, foi possível assistir a um aumento exponencial do recurso a métodos ocultos de investigação, fruto do progresso tecnológico. A criminalidade organizada e violenta tem vindo a evoluir substancialmente, ao que se junta a crescente ameaça do terrorismo, o fenómeno da globalização e a disseminação de novas tecnologias, que se afiguram como propícias para a redução da probabilidade da deteção da prática dos mais variados ilícitos. Perante estas novas capacidades adquiridas pelos meliantes de impossibilitar a deteção da prática de crimes, foi necessário recorrer a meios capazes de as contornar, por forma a atingir-se uma maior eficácia da investigação criminal.

O progresso tecnológico trouxe consigo inúmeras vantagens, tais como a abertura de um novo espaço de comunicação, a existência de comunidades virtuais e a facilidade e rapidez de partilha de informação. Todavia, o aparecimento de novas tecnologias não acarreta apenas benefícios, mas também malefícios significantes. Com a nova realidade virtual veio igualmente um novo conceito de criminalidade, a que tem lugar no ambiente digital. Os órgãos de polícia criminal deparam-se agora com um novo contexto, com a necessidade de terem de adaptar as suas investigações criminais a um novo espaço, repleto de especificidades.

Por forma a melhor combater este novo tipo de criminalidade, surgiu a Lei do Cibercrime, onde se encontram consagradas as ações encobertas em ambiente digital. Da atenta análise ao Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal, é possível concluir que não é concretizada uma qualquer distinção entre as ações encobertas em ambiente físico daquelas que decorrem em ambiente digital. Em boa verdade, sempre se dirá que este diploma legal foi desenhado para acautelar as especificidades das ações encobertas em ambiente físico, pois que, no momento da sua emanação, era a realidade que se apresentava como necessitada de tutela jurídica. Contudo, facilmente se compreende que as sociedades evoluem e, consequentemente, a criminalidade destas emergente também sofre um processo de evolução. Evolução esta que, atualmente, passa em grande parte pelo recurso a meios eletrónicos dos quais, à data da emanação do diploma em apreço, não havia muito conhecimento ou não eram alvo de tamanha utilização.

É nesta senda que surge a principal questão que se procura, com a presente dissertação de mestrado, abordar. Com efeito, atualmente assistimos a uma escassez, senão mesmo inexistência, de instrumentos legais especificamente dedicados à regulamentação das ações

encobertas em ambiente digital, aplicando-se nestes casos, analogicamente, as disposições existentes para as ações encobertas em ambiente físico. Todavia, por certa se terá a ideia de que investigar a prática de um crime em ambiente físico é totalmente diferente da atividade de investigação desenvolvida num ambiente digital. E, apesar de a aplicação por analogia das disposições relativas às ações encobertas em ambiente físico às que têm lugar em ambiente digital, decorrer sem problemas de maior, a verdade é que muitas especificidades destas últimas ficam por acautelar. Com efeito, é questionável até que ponto o Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal e as disposições relativas à interceção de comunicações tutelam devidamente a possibilidade de adoção de múltiplas identidades fictícias (inerente, a título de exemplo, à existência de vários perfis em redes sociais), a necessidade de conhecimentos técnicos por parte do agente encoberto, ou, ainda, o facto de estes vastos conhecimentos técnicos poderem levar a uma circunstância em que o agente encoberto tire proveito dos mesmos para encobrir a prática de crime da sua autoria.

A aplicação por analogia das disposições vigentes e, bem assim, a desconsideração destas especificidades poderá levar, em última *ratio*, a que estejamos perante um atropelo dos direitos fundamentais dos indivíduos alvos das ações encobertas e a uma falta de tutela jurídica que poderá culminar na nulidade da prova recolhida por intermédio deste meio de obtenção de prova.

Deste modo, esta é a questão que dá aso à presente dissertação – compreender se as especificidades inerentes à realização de ações encobertas em ambiente digital exigem a elaboração de um novo regime jurídico. Face ao problema que se afigura, tomamos por hipótese a possibilidade de elaborar um novo instrumento legal que, após o devido estudo de todas as particularidades das ações encobertas em ambiente digital, abarque e tutele devidamente o âmbito e condições de aplicação das mesmas.

1. PROVA EM PROCESSO PENAL

À semelhança do que sucede com qualquer outro processo, o processo penal traduz-se num conjunto de atos processuais encadeados entre si, tendo como objetivo apurar se uma determinada conduta poderá ser considerada como prática de um facto ilícito e se, no caso de uma resposta positiva, existe a possibilidade, ou não, de punir quem se vier a apurar ser o seu autor, podendo aqui ser aplicada uma pena ou uma medida de segurança. Poderá, assim, dizer-se que o processo penal se trata do "*(...) complexo orgânico de normas e leis relativas à realização prática do magistério penal e da proteção da inocência e da liberdade civil, mediante sentença que infunda na sociedade a confiança na justiça dos seus julgamentos."*[1].

Com efeito, não obstante se pretenda com o processo penal atingir uma decisão judicial, esta não poderá ser obtida de forma desmedida, sem olhar a meios para atingir um determinado fim. Torna-se necessário que o processo seja dotado de garantias, direitos e deveres que salvaguardem os interesses de todos os sujeitos processuais, sejam eles o arguido ou a vítima, e de verdadeiros princípios estruturantes que, em última análise, são indicadores do Estado de Direito e, bem assim, das normas jurídico-constitucionais ao mesmo inerentes.

Nesta senda, Jorge de Figueiredo Dias fala no direito processual penal como *direito constitucional aplicado*, numa dupla dimensão, entendendo que se que traduz "*(...) naquela, já caracterizada, derivada de os fundamentos do direito processual penal serem, simultaneamente, os alicerces constitucionais do Estado, e naquela outra resultante de a concreta regulamentação de singulares problemas processuais ser conformada jurídico-constitucionalmente.*"[2]. Do mesmo pensamento partilha Maria João Antunes, defendendo tratar-se o direito processual penal do *sismógrafo da Constituição de um Estado*, porquanto a estrutura e caracterização do processo penal depende das orientações políticas historicamente afirmadas[3]. O direito processual penal é, assim, uma verdadeira concretização do direito constitucional, na medida em que o âmago dos direitos dos cidadãos constitucionalmente consagrados, não poderá ser eliminado ou restringido por um qualquer instrumento legal, sem que para tal exista uma consciente e cuidada ponderação dos interesses em causa e uma regulamentação escrupulosa de possíveis intromissões. É da conformação jurídico-constitucional do direito processual penal que surge a expressão "*Diz-me como tratas o arguido, dir-te-ei o processo penal que tens e o Estado que o instituiu.*"[4].

---

[1] ANDRADE, Abel de, "Primeiras linhas de um Curso de Processo Penal", *In:* BELEZA, Teresa Pizarro; ISASCA, Frederico (Org.), *Direito Processual Penal - Textos*, Lisboa, Associação Académica da Faculdade de Direito de Lisboa, 1992, p. 216;
[2] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 74;
[3] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, p. 16.
[4] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 428;

Apesar de o processo penal apresentar uma intrínseca conexão com o direito constitucional, este não é o único ramo do Direito em que tal sucede, sendo que o mesmo se poderá afirmar relativamente ao direito penal. Entre ambos existe uma *relação mútua de complementaridade funcional*, cabendo, por um lado, ao direito penal, regulamentar os tipos de ilícitos e de culpa atinentes a cada crime e, cabendo, por outro, ao processo penal, concretizar tal regulamentação, disciplinando a investigação e esclarecimento do crime, que culminará na aplicação da competente sanção penal[5]. O direito penal efetiva-se por meio do processo penal, dado que é o primeiro que estipula quais os tipos legais de crime existentes e quais as consequências jurídicas a aplicar aos autores dos mesmos, mas é o segundo que determina como chegar à conclusão de que certo crime foi praticado, quem foi o seu agente e em que medida deverá ser-lhe aplicada uma sanção.

Como refere Germano Marques da Silva, a *unidade no mesmo pensamento funcional* estabelecida entre o direito penal e o processo penal não prejudica a existência de uma *autonomia específica* entre ambos, que resulta do facto de que, enquanto o direito penal tem como propósito o ordenamento da vida em sociedade, indicando quais os bens jurídicos merecedores de tutela, quais os comportamentos que os podem lesar e quais as sanções punitivas desses comportamentos; o processo penal visa disciplinar todo o procedimento tendente a verificar a ocorrência de um crime e a aplicar uma pena ou medida de segurança aos responsáveis pelo mesmo[6].

Neste sentido, entendem Mário Monte e Flávia Loureiro existir uma *autonomia teleológica* do direito processual penal, porquanto são vários os exemplos em que "*(...) o processo penal oferece uma solução para o conflito sem que esta esteja prevista no tipo legal de crime do Código Penal.*" e, nesta medida, o processo penal contribui "*(...) para a realização do direito penal, porque é através do processo que conseguimos soluções justas para os casos e, através da decisão judicativa do caso, o direito se realiza, se transforma a partir do conjunto de normas, de uma prescrição normativa, numa concretização da prescrição através da resolução de concretos casos jurídicos.*"[7].

Ademais, sempre se poderá dizer que o direito penal e o processo penal apresentam conteúdos e métodos diferentes. No que respeita ao conteúdo, as normas do direito substantivo determinam qual o valor e efeitos a atribuir a certas ações em geral; ao passo que as normas de

[5] *Idem*, pp. 27-28;
[6] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume I, 4ª edição, Editorial Verbo, 2000, pp. 16-17;
[7] MONTE, Mário Ferreira; LOUREIRO, Flávia Noversa, *Direito Processual Penal – Roteiro de aulas*, 2ª edição, Braga, AEDUM, 2014, p. 30.

direito adjetivo estabelecem o modo como as normas do direito substantivo podem ser aplicadas a casos concretos. Por outro lado, relativamente ao método, o direito penal apresenta um caráter especial e dedutivo; enquanto o processo penal comporta um caráter crítico e indutivo[8].

Intimamente ligado ao direito penal e ao processo penal, encontra-se, de igual modo, o direito da execução de penas, sendo estes três setores de um *idêntico ordenamento jurídico* [9], uma vez que entre si formam o direito penal em sentido amplo, parte integrante da denominada *ciência total do direito penal*, a par da criminologia e da política criminal[10]. Ao direito da execução de penas cumpre a função de regulamentar juridicamente a execução das penas e medidas de segurança que foram determinadas pela decisão judicial proferida no âmbito do processo penal. Contudo, este ramo do direito não se confunde com o processo penal, na medida em que, apesar de encontrarmos normas de caráter adjetivo, as mesmas são relativas à realização concreta do conteúdo da sentença condenatória proferida[11].

Ora, conforme resulta da definição *supra* transcrita e analisada, o processo penal tem como objetivo compreender se foi, efetivamente, praticado algum tipo legal de crime, quem foi o seu autor e se ao mesmo deve ser aplicada uma pena ou medida de segurança. De acordo com os ensinamentos de Figueiredo Dias, desta noção pode retirar-se a conclusão de que são várias as finalidades inerentes ao processo penal, como sejam a realização da justiça e a descoberta da verdade material; a proteção dos direitos fundamentais dos cidadãos; e, por último, o restabelecimento da paz jurídica.

Sucede, contudo, que estas finalidades do processo penal não são, na prática, integralmente harmonizáveis, porquanto para se dar efetividade plena a uma é, por vezes, necessário colocar em causa outra. Nestes casos, o autor entende ser essencial operar uma *concordância prática* entre todas as finalidades, onde possa ser possível obter o máximo de conteúdo de cada uma e, ao mesmo tempo, minimizar-se as perdas funcionais que inevitavelmente irão ocorrer[12]. Ocorrerá, assim, uma "*(...) mútua compressão das finalidades em conflito por forma a atribuir a cada uma a máxima eficácia possível (...)*"[13].

Várias têm sido as decisões proferidas pela jurisprudência dos tribunais superiores, acerca da aplicação desta *concordância prática*, nomeadamente o Acórdão n.º 607/2003 do Tribunal

[8] ANDRADE, Abel de, "Primeiras linhas de um Curso de Processo Penal", In: BELEZA, Teresa Pizarro; ISASCA, Frederico (Org.), *Direito Processual Penal - Textos, Lisboa*, Associação Académica da Faculdade de Direito de Lisboa, 1991/1992, p. 194;
[9] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 27;
[10] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, p. 7;
[11] *Idem*, pp. 7-10;
[12] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, pp. 30-40;
[13] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, p. 15.

Constitucional, onde se pode ler, a respeito da valoração de um diário como meio de prova, que "*A Constituição não exclui que, neste domínio específico, uma ponderação possa conduzir a que, em concreto, o interesse público geral na investigação dos ilícitos penais imputados ao arguido e na prossecução da verdade material e a subsequente realização da justiça se sobreponham, acauteladas as devidas reservas, às necessidades de tutela da sua esfera de privacidade, não sendo assim de afastar, dentro do domínio tido por admissível, uma valoração das descrições constantes de diários em processo penal, conquanto esta não se mostre desadequada, desnecessária e desproporcionada face aos valores e ao tipo de decisão em causa*"[14].

Cumpre, ainda, atentar que, o modo como os direitos e deveres dos sujeitos processuais são efetivados no âmbito do processo penal depende da estrutura pelos Estados adotada quanto a este. Ao longo da história foi possível identificar dois grandes modelos de estrutura do processo penal, a saber: a estrutura acusatória e a estrutura inquisitória.

O modelo de estrutura acusatória tem como principal fundamento a separação entre a entidade que investiga/acusa e a entidade que julga, pretendendo com a mesma atingir uma total imparcialidade do julgador. Ocorre, no seio do mesmo, uma confrontação entre a acusação e a defesa, com respeito pelos princípios do contraditório e da igualdade de armas, o que leva, inevitavelmente, não a uma verdade material, mas sim a uma verdade processual. Às partes cabe toda a produção de prova, em cumprimento da distribuição do ónus da prova, sendo vedada ao juiz qualquer iniciativa relacionada com mesma[15].

Por outro lado, no modelo de estrutura inquisitória assistimos a uma concentração dos poderes de investigação, acusação e julgamento numa só entidade – o juiz. Existe uma total desconsideração pelas garantias e direitos do arguido, procurando obter-se, a todo o custo, a realização da justiça e a descoberta da verdade material. Conforme refere Germano Marques da Silva, "*No sistema inquisitório o juiz, agora magistrado profissional, intervém ex officio, sem necessidade de acusação, investiga oficiosamente com plena liberdade na recolha das provas, pronuncia e julga com base nas provas por si recolhidas; o juiz é o dominus do processo e o suspeito praticamente não tem direitos processuais frente ao juiz*."[16].

Em Portugal, o processo penal foi adotando diferentes modelos até chegar ao atualmente consagrado. Com efeito, o Código de Processo Penal de 1929 traduzia um modelo de estrutura acusatória formal, que, na prática, se traduzia numa estrutura inquisitória, porquanto, apesar de

[14] Acórdão n.º 607/203, de 5 de Dezembro, relativo ao processo n.º 594/03, disponível em https://bityli.com/f4jSl, último acesso em 14-03-2022;
[15] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 27;
[16] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume I, 4ª edição, Editorial Verbo, 2000, p. 59.

ser o Ministério Público a investigar e a acusar, cabia ao mesmo juiz tanto a instrução como o julgamento[17]. Posteriormente, a introdução da atual redação do n.º 5 no artigo 32.º da Constituição da República Portuguesa veio consagrar a estrutura acusatória do processo penal português, estando, no entanto, a audiência de julgamento e os atos instrutórios que a lei determinar subordinados ao princípio do contraditório. Esta validação do modelo de estrutura acusatória revelou-se o início de uma grande inovação e reforma do processo penal até então vigente.

No entendimento de Figueiredo Dias, o preceito constitucional *supra* aludido reveste uma magna importância, sendo mesmo, para si, a mais importante de todas as normas constitucionais respeitantes ao processo penal. Defende, nesta senda, que "*Esta norma (...) serve de fundamento à construção de um direito processual penal de futuro: de um direito processual penal que há-de potenciar a participação construtiva dos sujeitos processuais na finalidade e no objeto do processo, ao mesmo tempo que levantar um veto terminante a qualquer veleidade de regresso a ideias típicas do processo inquisitório*;"[18].

Para que se pudesse dar execução ao referido preceito constitucional, foi pelo Governo solicitada autorização para aprovar o Código de Processo Penal atualmente vigente, tendo a mesma sido concedida sob forma da Lei n.º 43/86, de 26 de Setembro, e dadas indicações no sentido de simplificar a tramitação processual, aumentar a igualdade de armas material, definir rigorosamente o momento e modo de obtenção do estatuto processual de arguido, garantir a liberdade de atuação do defensor em todo o processo, entre outros[19].

Desta forma, nos dias de hoje, o processo penal português adota um modelo de estrutura acusatória integrado por um princípio de investigação, de acordo com o qual o inquérito é dominado pelo Ministério Público e tem uma natureza predominantemente inquisitória, não sabendo o arguido quais as provas que foram contra si recolhidas. Ao Ministério Público cabe igualmente a tarefa de acusar ou arquivar o inquérito caso tenha, ou não, descoberto indícios suficientes da prática de um crime e de quem foi o seu autor. Na fase facultativa de instrução e,

---

[17] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, p. 20;

[18] DIAS, Jorge de Figueiredo, "O Novo Código de Processo Penal", In: BELEZA, Teresa Pizarro; ISASCA, Frederico (Org.), *Direito Processual Penal - Textos, Lisboa*, Associação Académica da Faculdade de Direito de Lisboa, 1991/1992, p. 18;

[19] Cfr. alíneas 2, 4, 8 e 9 do n.º 2 do artigo 2.º da Lei n.º 43/86, de 26 de Setembro:
"*2 - A autorização referida no artigo anterior tem o seguinte sentido e extensão:*
2) Simplificação, desburocratização e aceleração da tramitação processual compatíveis com a realização das finalidades assinaladas, evitando-se todavia a criação de novos formalismos inúteis;
4) Estabelecimento da máxima acusatoriedade do processo penal, temperada com o princípio da investigação judicial;
8) Definição rigorosa do momento e do modo de obtenção do estatuto de arguido, com carácter irreversível e concomitante estatuição da obrigatoriedade para as autoridades judiciárias e de polícia criminal de explicitarem os direitos e deveres inerentes a tal qualidade;
9) Garantia efetiva da liberdade de atuação do defensor em todos os atos do processo, sem prejuízo do carácter não contraditório da fase de inquérito preliminar; em especial, garantia do direito de estar presente a todo e qualquer interrogatório do arguido, bem como o de conferenciar com este em qualquer momento do processo, salvo quando se trate de casos de terrorismo, criminalidade violenta ou altamente organizada, hipótese em que só poderá fazê-lo a seguir ao primeiro interrogatório feito pelo juiz de instrução.".

ainda, na fase de julgamento, vigora o princípio da igualdade de armas, não podendo o juiz que presidiu à instrução ser o mesmo que julga. Apesar de o juiz se encontrar adstrito à prova recolhida em sede de investigação pelo Ministério Público e, posteriormente, produzida em sede de instrução ou julgamento, ao mesmo é ainda atribuída a faculdade de ordenar oficiosamente a produção de todos os meios de prova que entenda por necessários para a boa decisão da causa.

A imparcialidade e independência do julgador é uma característica bastante presente no modelo de estrutura de processo penal atualmente adotado entre nós, e algo que se procura sempre alcançar. Tal é visível no facto de, a título de exemplo, a prova produzida em sede de inquérito e instrução ter de ser, novamente, produzida em sede de julgamento, porquanto o juiz que agora julga a causa não assistiu à produção da prova nas fases anteriores e, caso não ocorresse uma produção de prova *ex novo* em sede de julgamento, o mesmo estaria a ser condicionado, afetando assim, manifestamente a sua isenção e imparcialidade[20]. Cumpre, de igual modo, realçar que, a despeito de terem de ser carreados para o processo penal todos os elementos probatórios que permitam a demonstração da ocorrência de um crime e de quem foi o seu agente, não existe um verdadeiro ónus da prova, pelo que inexiste a obrigação de quem alega/invoca determinado facto, ter que fazer prova do mesmo. Contudo, sempre se dirá que, a falta de produção de prova, terá como consequência necessária a absolvição do arguido, na esteira do princípio da presunção de inocência.

Conforme resulta do vindo de expor, a prova assume um papel preponderante no que respeita à efetivação do processo penal e das suas finalidades, na medida em que, sem a mesma, não se torna possível punir o agente de um crime e, bem assim, proteger os direitos fundamentais dos cidadãos, restabelecer a paz jurídica e realizar a justiça. Contudo, não se pode dar aso a uma produção de prova desmedida e desregrada. Torna-se, pelo contrário, necessário conhecer todas as suas características e vicissitudes, nomeadamente todas as barreiras que, uma vez ultrapassadas, nos colocam no campo da prova ilícita e obtida através de meios ilegais.

1.1. Conceito de Prova

Ao longo da história, vários têm sido os conceitos de prova avançados pelos diferentes autores. Não obstante o Código de Processo Penal não avance com um conceito devidamente limitado para a prova, o Código Civil, no seu artigo 341.º, relaciona o conceito de prova com a atividade de demonstração da realidade dos factos alegados em juízo. Tal demonstração irá

[20] MONTE, Mário Ferreira; LOUREIRO, Flávia Noversa, *Direito Processual Penal – Roteiro de aulas*, 2ª edição, Braga, AEDUM, 2014, p. 64.

desempenhar um papel de extrema importância no que diz respeito ao modo como o processo penal irá terminar. Isto é, a efetiva existência, ou não, de prova, vai influenciar profundamente o conteúdo da decisão judicial a ser proferida, na medida em que a sua presença culminará na aplicação de uma pena ou medida de segurança ao arguido e, a sua ausência, determinará a absolvição do mesmo, na senda do princípio *in dubio pro reo*.

Esta demonstração da realidade dos factos, no entendimento de Cavaleiro de Ferreira, encontra-se diretamente relacionada com a ideia de alcançar um juízo de certeza sobre os factos em apreço, juízo de certeza este que poderá assumir a forma de juízo lógico ou juízo histórico. Neste seguimento, "*O juízo lógico respeita à exatidão dum raciocínio, duma operação mental; conduz necessariamente a uma certeza absoluta. O juízo histórico respeita à verificação dum facto, e por isso mesmo, pode não conduzir a um resultado seguro; não acarreta uma certeza absoluta, mas relativa, não uma certeza objetiva, mas uma opinião de certeza.*"[21].

Fernando Gonçalves e Manuel Alves entendem, numa primeira aceção, traduzir-se a prova numa atividade que irá produzir no julgador da causa uma convicção sobre a veracidade, ou não, de uma determinada afirmação. Todavia, alertam para o facto de a expressão *prova* não significar apenas uma atividade probatória, mas igualmente dizer respeito à matéria dos meios de prova[22]. Por seu turno, Manuel Guedes Valente defende que o instituto da prova revela muito mais do que um simples conceito fixo positivo, porquanto apresenta uma dimensão e natureza poliédrica. Para este autor, "*A prova, enquanto instituto jurídico do Direito, assume uma conceção de natureza jurídica poliédrica: tem várias faces e cada face gera um conceito próprio que assenta na tetrateleologia do processo penal (...) subsumida ao princípio da concordância prática.*" – sendo esta tetrateleologia a descoberta da verdade; a realização da justiça; a defesa e garantia dos direitos de todos os cidadãos; e o restabelecimento da paz jurídica e social[23].

Cumpre igualmente esclarecer, no que concerne ao caráter polissémico da palavra *prova*, a frequente distinção efetuada entre prova enquanto atividade probatória, enquanto resultado da atividade probatória e enquanto meio de prova. Enquanto atividade probatória, a prova é "*(...) o esforço metódico através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis.*"[24]. Já enquanto resultado da atividade probatória, traduz-se na "*(...) motivação da*

[21] FERREIRA, Manuel Cavaleiro de, *Curso de Processo Penal*, Volumes I e II, Lisboa, Lições proferidas no ano letivo 1954-1955, pp. 280-281;
[22] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 123;
[23] VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Almedina, 2019, p. 18.
[24] MENDES, Paulo de Sousa, "As Proibições de Prova no Processo Penal", *In*: Faculdade de Direito da Universidade de Lisboa e Conselho Distrital de Lisboa da Ordem dos Advogados (Org.), *Jornadas de Direito Processual Penal e Direitos Fundamentais*, coordenação científica de Maria Fernanda Palma, Almedina, 2004, p. 133;

convicção da entidade decidente acerca da ocorrência dos factos relevantes, contanto que essa motivação se conforme com os elementos adquiridos representativamente no processo e respeite as regras da experiência, as leis científicas e os princípios da lógica."[25]. Por fim, enquanto meio de prova, temos "*(...) os elementos com base nos quais os factos relevantes podem ser demonstrados*."[26].

Uma vez compreendido o conceito de prova e todas as aceções do mesmo, importa atentar sobre o que versa a mesma, isto é, qual o objeto da prova. O artigo 124.º do Código de Processo Penal esclarece que objeto da prova serão todos os factos juridicamente relevantes para a existência do crime, a punibilidade do agente e a determinação da sanção penal a aplicar, sendo que aqui se incluem igualmente os factos atinentes à responsabilidade civil, caso seja deduzido o competente pedido de indemnização cível[27]. A noção de *factos juridicamente relevantes* compreende, não só os factos atinentes aos aspetos *supra* mencionados, como também os factos pertinentes para o proferimento de decisões prévias, interlocutórias ou incidentais, que sucedem no decorrer do processo penal, nomeadamente a aplicação de medidas de coação ou de garantia patrimonial[28].

Sendo o objeto da prova os factos juridicamente relevantes para os vários aspetos do processo penal, o fim ou a finalidade da mesma será necessariamente a demonstração da realidade dos mesmos, conforme já aludido *supra*. Contudo, não se poderá afirmar que esta é a única finalidade da prova. Germano Marques da Silva realça que, para além desta demonstração da realidades dos factos, "*A prova, entendida como atividade probatória, é também garantia de realização de um processo justo, de eliminação do arbítrio, quer enquanto a demonstração da realidade dos factos não há-de procurar-se a qualquer preço, mas apenas através de meios lícitos, quer enquanto através da obrigatoriedade de fundamentação das decisões de facto permite a sua fiscalização através de diversos mecanismos de controlo de que dispõe a sociedade*."[29].

De igual modo, no que ao papel da prova no nosso processo penal diz respeito, podemos afirmar que esta é *fundamento, fim e limite do Direito* [30]. Numa dimensão de fundamento, a prova pressupõe a existência de um facto, facto este que a lei penal qualifica como um tipo legal de

---

[25] *Ibidem*;
[26] *Ibidem*;
[27] Cfr. n.º 1 e 2 do artigo 124.º do Código de Processo Penal:
"*1 - Constituem objeto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis.*
2 - Se tiver lugar pedido civil, constituem igualmente objeto da prova os factos relevantes para a determinação da responsabilidade civil.";
[28] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 125.
[29] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, pp. 110-111;
[30] VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Almedina, 2019, p. 20;

crime e que justifica a intervenção dos órgãos de polícia criminal, nomeadamente no que concerne à recolha de indícios e vestígios probatórios; numa dimensão de fim, a prova traduz-se num elemento central do direito penal adjetivo, porquanto a esta são associadas as finalidades do próprio processo penal, como sejam a descoberta da verdade material e a realização da justiça; por último, numa dimensão de limite, temos o princípio da limitabilidade probatória, de acordo com o qual não é possível valorar as provas que foram obtidas de uma forma ilícita e contrária aos limites estabelecidos pelo Estado de Direito democrático[31].

No que respeita à questão probatória, à sua finalidade de demonstração da realidade dos factos e ao consequente fim do processo penal de descoberta da verdade material, assistimos frequentemente à dicotomia entre verdade real e verdade processual. Com efeito, o que se assiste no processo penal é a uma reprodução de factos passados, uma reconstituição de uma situação que teve o seu início e fim num momento anterior ao do processo, pelo que, qualquer verdade que possa vir a alcançar no seio deste, será uma verdade meramente processual, dado que a verdade real já se esgotou aquando da ocorrência dos factos em apreço.

No processo penal, a verdade tem por objeto uma *aproximação metodológica à realidade*, na medida em que não estamos no campo da certeza mas sim da probabilidade[32]. Conforme refere Cavaleiro de Ferreira, a prova não leva à certeza objetiva e absoluta. Pelo contrário, a única meta ao alcance do Homem é a verdade relativa, em sentido subjetivo, equivalente à máxima probabilidade, ocupando, assim, a certeza subjetiva o lugar de verdade material no âmbito do processo penal. Impõe-se, neste conspecto, ao julgador, que percorra com extrema prudência todo o caminho que levará à formação da sua convicção acerca dos factos apresentados em pleito, porquanto a falta da mesma poderá fazer o juiz incorrer em erros de julgamento que, por sua vez, poderão trazer graves consequências para os vários agentes processuais[33] [34].

Para Germano Marques da Silva, esta verdade processual que se atinge "*(...) não é senão o resultado probatório processualmente válido, isto é, a convicção de que certa alegação singular de facto é justificavelmente aceitável como pressuposto da decisão, por ter sido obtida por meios*

---

[31] *Idem*, pp. 21-23;

[32] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 124.

[33] FERREIRA, Manuel Cavaleiro de, *Curso de Processo Penal*, Volumes I e II, Lisboa, Lições proferidas no ano letivo 1954-1955, pp. 281-282;

[34] Neste sentido, vide TARUFFO, Michele, *La Prueba, Artículos y Conferencias*, Monografias Jurídicas Universitas, Editorial Metropolitana, p. 68, disponível em https://bityli.com/HNYv9: "*Sin embargo, no se duda, a pesar de estos límites, de que la búsqueda de la verdad tiene sentido y que un decisor racional debe tender a maximizar la verdad de su conocimiento sobre los hechos que le interesan, si quiere maximizar la validez de sus decisiones y reducir el riesgo de errores que puedan traer graves consecuencias.*", e DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 204: "*Certo é que, como já se notou, a verdade 'material' que se busca em processo penal não é o conhecimento ou apreensão absolutos de um acontecimento, que todos sabem escapar à capacidade de conhecimento humano; tanto mais que aqui intervêm, irremediavelmente, inúmeras fontes possíveis de erro, quer porque se trata do conhecimento de acontecimentos passados, quer porque o juiz terá as mais das vezes de lançar mão de meios de prova que, por sua natureza (...) se revelam particularmente falíveis.*";

processualmente válidos. A verdade processual não é absoluta nem ontológica, mas uma verdade judicial, prática e, sobretudo, não uma verdade obtida a todo o preço mas processualmente válida."[35]. Assim, a descoberta da verdade no âmbito do processo penal será sempre norteada pelas regras probatórias estabelecidas, o que implica um respeito total pelos direitos fundamentais dos cidadãos. Tal respeito, aliado às regras gerais do conhecimento, na medida em que este é necessariamente limitado, conduzem à conclusão clara de que, para garantir este respeito, apenas se chegará a uma verdade relativa, isto é, processual, sendo a verdade real ou absoluta impossível de alcançar.

Conforme já *supra* exposto, para que o tribunal possa formar a sua convicção e, posteriormente, proferir a decisão judicial final, deverá percorrer todo um caminho, caminho este que deverá ter em atenção as regras probatórias em vigor. Sucede que, estas regras probatórias variam consoante o sistema de apreciação e valoração de prova adotado, identificam-se, ao longo dos anos, maioritariamente dois sistemas, a saber: o sistema da prova legal ou tarifada e o sistema da prova livre ou da livre apreciação da prova.

Com efeito, apesar de nos dias de hoje já assim não ser, até ao final do século XVIII, vigorava na generalidade dos países o sistema da prova legal ou tarifada, de acordo com o qual existia uma predeterminação legislativa, específica e taxativa, de quais os meios de prova que poderiam ser utilizados para formar a convicção do julgador. Existia um verdadeiro *numerus clausus* dos meios de prova admitidos, com a intenção de limitar ao máximo a discricionariedade que pudesse ser exercida pelos juízes, na medida em que o legislador determinava antecipadamente quando e como deveriam ser provados os factos trazidos a juízo, vinculando o valor da prova[36].

Contudo, com a Revolução Francesa, iniciada 1789, assistimos a uma mudança de paradigma. O sistema de prova legal foi substituído por um sistema de prova livre, atualmente em vigor em Portugal, na senda do qual os meios de prova deixaram de ter um valor aferido *a priori*, inexistindo, assim, critérios legais predeterminados acerca do valor a atribuir à prova[37]. Neste seguimento, passou a escrever-se no artigo 125.º do Código de Processo Penal que "*São admissíveis as provas que não forem proibidas por lei.*", significando este preceito legal que, não são apenas os meios de prova tipificados que são admitidos, mas sim todos os que, mesmos não tipificados ou previstos legalmente, não sejam proibidos por lei.

[35] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, pp. 130.
[36] *Idem*, p. 137;
[37] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 202;

Desta forma, passamos de um sistema onde o julgador se encontrava vinculado a regras sobe a apreciação da prova já previamente estabelecidas para um sistema onde o mesmo dispõe de discricionariedade, devendo atender apenas à lógica e às máximas da experiência[38]. Cumpre, todavia, ressalvar que, conforme apontado por Cavaleiro de Ferreira, "*A predeterminação legal do valor das provas, prendendo a decisão judicial em matéria de facto a regras fixas tinha de conduzir algumas vezes a resultados contraditórios com a consciência individual e convicção do julgador. O desaparecimento destas restrições à livre convicção não acarreta, porém, uma facultade arbitrária de decidir. (...) A livre convicção é um meio de descoberta da verdade, não uma afirmação infundamentada da verdade. É uma conclusão livre, porque subordinada à razão e à lógica e não limitada por prescrições formais exteriores. (...) Simplesmente o julgador em vez de se encontrar ligado por normas prefixadas e abstratas sobre a apreciação da prova, tem apenas de se subordinar à lógica, à psicologia e às máximas da experiência.*"[39]. A atuação do juiz não passa, assim, a ser totalmente desregrada, apenas lhe é atribuída uma maior liberdade no que diz respeito ao valor a atribuir à prova.

A estrutura de processo penal entre nós adotada, isto é, uma estrutura acusatória mitigada pelo princípio da investigação, combinada com o sistema adotado de prova livre implica que, não só os sujeitos processuais têm o direito a participar de forma ativa na produção de prova, como deve o tribunal, igualmente, procurar recorrer a provas que não as já apresentadas, quando assim se afigurar necessário, para a melhor decisão da causa de acordo com as regras da experiência.

1.2. Princípios processuais relativos à prova

Importa, no seguimento do que vem sido exposto, atentar nos princípios enformadores do processo penal, mormente os relativos à prova. O estudo dos mesmos não deve ser, de todo, descartado, na medida em que são excelentes indicadores dos valores fundamentais que são a base do processo penal vigente, assim como das opções políticas e legislativas adotadas, que, em última análise, dão a mostrar os aspetos essenciais e dominantes de uma determinada sociedade. De igual modo, os princípios gerais do processo penal desempenham, nos termos do disposto no artigo 4.º do Código de Processo Penal, um importante papel no que respeita à integração de

[38] Cfr., neste sentido, o douto aresto do Tribunal da Relação de Évora, datado de 30-01-2007, relativo ao processo n.º 2457/06-1, disponível em https://bityli.com/FBoYk, último acesso em 15-03-2022, onde se pode ler que "*Contrariamente aos sistemas de prova legal, o modelo caracterizado pelo princípio da livre apreciação da prova implica sobretudo que o juiz não se encontre sujeito a regras, prévia e legalmente fixadas sobre o modo como deve valorar a prova, libertando-o das regras rígidas da prova tarifada.*";

[39] FERREIRA, Manuel Cavaleiro de, *Curso de Processo Penal*, Volumes I e II, Lisboa, Lições proferidas no ano letivo 1954-1955, p. 298.

lacunas, sendo estes os aplicados quando não for possível aplicar as normas do referido texto normativo por analogia ou as normas de processo civil que se harmonizem com o processo penal. Iremos, assim, atentar nos princípios do processo penal atinentes à matéria da prova, como sejam o princípio da oralidade, da imediação, da concentração, da investigação ou verdade material, do contraditório, da livre apreciação da prova, da presunção de inocência e *in dubio pro reo*.

O princípio da oralidade do processo penal determina que, em especial no que se reporta à produção de prova em audiência de discussão e julgamento, a mesma ocorra de forma oral e na presença dos sujeitos processuais. Este princípio advém da publicidade caracterizadora do processo penal, porquanto o público apenas consegue acompanhar a prática dos diversos atos processuais se os mesmos foram realizados de forma oral. Tal não significa que a prática oral destes atos não possa vir a ser documentada, muito pelo contrário, esta documentação deve ocorrer, com o intuito de permitir um maior controlo da prova, relevante para efeitos de interposição de recursos jurisdicionais. Com previsão legal no n.º 1 do artigo 96.º do Código de Processo Penal, o princípio da oralidade apresenta como vantagem o favorecimento da descoberta da verdade material, uma vez que o diálogo, a possibilidade de observar as reações dos sujeitos processuais e as suas respostas espontâneas facilita esta tarefa; e como desvantagem a subjetividade desta oralidade. O respeito pelo princípio da oralidade permite, assim, um contacto direto e imediato do tribunal com as provas[40], devendo este, aquando do proferimento da decisão final, ter em conta a produção de prova oral ocorrida em sede de audiência de discussão e julgamento[41].

Intimamente ligado ao princípio da oralidade, encontra-se o princípio da imediação, que, de acordo com a noção avançada por Jorge de Figueiredo Dias, se pode definir como "*(...) a relação de proximidade comunicante entre o tribunal e os participantes no processo, de modo tal que aquele possa obter uma perceção própria do material que haverá de ter como base na sua decisão.*"[42]. Este princípio, previsto no artigo 355.º do Código de Processo Penal, pressupõe um contacto imediato com os meios de prova em geral[43], sendo que a decisão final apenas poderá ser proferida por quem tenha assistido à totalidade da produção de prova e à discussão dos factos em causa, dando-se preferência aos meios de prova que se encontrem numa relação mais direta

[40] JESUS, Francisco Marcolino de, *Os Meios de Obtenção da Prova em Processo Penal*, Almedina, 2011, p. 103.

[41] Vide, neste sentido, o acórdão do Supremo Tribunal de Justiça, datado de 14-03-2007, relativo ao processo n.º 07P21, disponível em https://bityli.com/NJOyC, último acesso em 15-03-2022, no qual se pode ler que: "*Quando se fala da "oralidade" como princípio geral do processo penal tem-se em vista a forma oral de atingir a decisão: o processo será dominado pelo princípio da escrita quando o juiz profere a decisão na base de atos processuais que foram produzidos por escrito (atas, protocolos, etc.); será, pelo contrário, dominado pelo princípio da oralidade quando a decisão é proferida com base numa audiência de discussão oral da matéria a considerar.*";

[42] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 232;

[43] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, pp. 178-179;

com tais factos[44]. Esta exigência de relação de proximidade entre os intervenientes processuais e o tribunal cumpre-se numa dimensão física e temporal, daí que seja de extrema importância a presença dos mesmos na audiência de discussão e julgamento[45].

Igualmente relacionado com ambos os princípios *supra* mencionados, o princípio da concentração determina que todos os atos a praticar no âmbito do processo, em sede de audiência de discussão e julgamento, devem sê-lo em apenas uma única audiência ou, quando tal não seja possível, em várias com a maior proximidade temporal possível. Equacionado nos artigo 328.º e 365.º n.º 1 do Código de Processo Penal, este princípio desdobra-se em duas vertentes distintas: uma vertente de concentração espacial, de acordo com a qual a audiência de discussão e julgamento deve decorrer, na sua íntegra, num mesmo espaço; e uma vertente de concentração temporal, na senda da qual, a audiência deve decorrer de forma contínua até ao seu encerramento, salvo casos em que, mediante despacho fundamentado, a mesma seja objeto de interrupções ou adiamentos. No que concerne à importância deste princípio, Mário Monte e Flávia Loureiro alertam para a circunstância de que "*Exige-se esta concentração, porque, por um lado, no que diz respeito à continuidade temporal, a sua inexistência provoca uma certa falta de celeridade, a qual é importante para garantir que o efeito útil da decisão seja o maior possível. Depois. Para garantir a eficácia dos atos processuais, pois que, se há uma certa sequência de atos e se há uma quebra temporal, isso faz com que haja uma quebra no próprio conhecimento e, por vezes, o hiato temporal é tão grande que implica que se volte a repetir o ato.*"[46].

Por seu turno, o princípio da investigação ou da verdade material encontra-se consagrado no n.º 1 do artigo 340.º do Código de Processo Penal, de acordo com o qual "*O tribunal ordena, oficiosamente ou a requerimento, a produção de todos os meios de prova cujo conhecimento se lhe afigure necessário à descoberta da verdade e à boa decisão da causa.*"[47]. O mesmo é dizer que, conforme já *supra* aludido, num processo penal de estrutura acusatória, mitigada por este mesmo princípio, recai, em última instância, sobre o tribunal, o ónus de investigar, de modo oficioso, os factos submetidos a juízo. Pretende-se, assim, alcançar a verdade material, que poderá

---

[44] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume I, 4ª edição, Editorial Verbo, 2000, p. 90;

[45] Vide, neste sentido, o acórdão do Tribunal da Relação de Coimbra, datado de 21-11-2001, relativo ao processo n.º 926/2001, disponível em https://bityli.com/aW1hl, último acesso em 15-03-2022, no qual se pode ler que: "*A imediação que vem definida como a relação de proximidade comunicante entre o tribunal e os participantes no processo, de tal como que, em conjugação com a oralidade, se obtenha uma perceção própria dos dados que haverão de ser a base da decisão. É pela imediação, também chamado de princípio subjetivo, que se vincula o juiz à perceção, à utilização, à valoração e credibilidade da prova.*"; e, ainda, o douto aresto n.º 394/89 do Tribunal Constitucional, datado de 18-05-89, disponível em https://bityli.com/twkVP, último acesso em 15-03-2022, sendo explícito no mesmo que: "*Mas, a presença do arguido na audiência é também essencial para a averiguação da verdade material e para que o juiz possa conhecer o arguido: Só através da imediação da prova, o juiz pode olhar o argui-do, fazer dele o seu retrato, ter a perceção direta do seu modo de ser, a verdadeira imagem do sujeito, da pessoa que de facto vai julgar como agente de um facto criminoso.*".

[46] MONTE, Mário Ferreira; LOUREIRO, Flávia Noversa, *Direito Processual Penal – Roteiro de aulas*, 2ª edição, Braga, AEDUM, 2014, p. 162.

[47] Vide, igualmente, no que concerne ao princípio da investigação ou verdade material os artigos 154.º n.º 1, 164.º n.º 2, 174.º n.º 3, 288.º n.º 4, 289.º n.º 1, 290.º n.º 1, 348.º n.º 5 e 354.º, todos do Código de Processo Penal;

ser equacionada num duplo sentido: uma verdade que seja imune às influências que, tanto a acusação como a defesa, exercem sobre ela; e uma verdade meramente judicial, processualmente válida, não obtida mediante o desrespeito pelos direitos fundamentais dos cidadãos e, por isso, não uma verdade absoluta, como já analisado anteriormente[48].

Com a consagração deste princípio, sendo necessário para a descoberta da verdade e boa decisão da causa, o tribunal pode e deve recorrer a outros meios de prova que não os já apresentados pelas partes no processo, implicando tal a não existência de um ónus da prova sobre as mesmas. Contudo, tal entendimento não é totalmente pacífico. Na verdade, Paulo de Sousa Mendes entende existir várias incompreensões relativamente à existência de ónus da prova em processo penal. De acordo com a tese defendida por este autor, "*(...) é correto dizermos que a acusação, não o MP ou o acusador particular, tem um ónus material (objetivo) de produzir meios de prova (ónus de produção) e de persuadir o tribunal de que as provas são bastantes para a condenação do arguido (ónus de persuasão) (...). Só que o MP não tem um ónus subjetivo, quer dizer: não tem interesse na condenação do arguido a qualquer preço, pois protagoniza apenas o interesse público na descoberta da verdade e na realização da justiça.*"[49]. Independentemente das querelas doutrinárias que possam existir, mormente as relativas à temática do ónus da prova, o princípio da investigação ou da verdade material é claro: o tribunal não deverá contentar-se se, da prova produzida em todo o processo, resultar a dúvida relativa à realidade dos factos alegados; pelo contrário, deverá procurar ultrapassar essa mesma dúvida, sempre na medida do possível[50].

Não obstante, os poderes de investigação atribuídos ao juiz não podem adquirir um caráter ilimitado. Com efeito, tal como alerta Ana Raquel Conceição, os referidos poderes têm que se adequar aos direitos de defesa do arguido, o que leva à imposição de que os mesmos sejam limitados a partir de dado momento no processo. Com a formulação da acusação, o objeto do processo fica delimitado e não é permitido ao juiz conhecer novos factos que alterem substancialmente o mesmo. Um outro entendimento levaria a uma situação insustentável para o arguido, onde, a qualquer momento poderia ser confrontado com novos factos e, bem assim, ver-se obrigado a alterar a sua defesa[51].

Ora, apesar de caber ao julgador procurar, ativa e oficiosamente, a produção de prova dos factos trazidos a juízo, a verdade é que não o deve fazer de modo solitário, deve antes ouvir as diferentes partes, acusação e defesa. E é nesta senda que surge o princípio do contraditório, nos

[48] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 144.
[49] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 217;
[50] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, p. 130;
[51] CONCEIÇÃO, Ana Raquel, *Escutas Telefónicas – Regime Processual Penal*, Lisboa, Quid Iuris, 2009, p. 44;

termos do qual, antes de proferir as suas decisões, deve o tribunal ouvir a acusação e a defesa, e dar-lhes a possibilidade de se pronunciarem acerca das condutas processuais que a contraparte possa adotar. Com consagração no n.º 5 do artigo 32.º da Constituição da República Portuguesa, o princípio do contraditório apenas vê a sua total aplicação em sede de audiência de discussão e julgamento e em determinados atos instrutórios, quando a lei nesse sentido dispuser, o que implica que as fases de inquérito e instrução, na sua generalidade, não estão necessariamente sujeitas a este princípio.

No que respeita à relação deste princípio com a posição de arguido, cumpre esclarecer que o mesmo integra o estatuto processual deste, com respaldo nas alíneas a), b) e g) do n.º 1 do artigo 61º do Código de Processo Penal[52], tendo a jurisprudência do Tribunal Constitucional vindo a entender que, relativamente à violação deste princípio, "*Só ocorre violação dos princípios constitucionais pertinentes, mormente do princípio do contraditório, se as partes ficarem impossibilitadas de controlar as (e, portanto, de responder às) questões colocadas pelo Ministério Público aquando da sua intervenção no processo, o que naturalmente não acontece, sempre que de tal intervenção não decorra qualquer questão nova, ainda não conhecida das partes e, portanto, por elas ainda não respondida.*"[53].

O princípio da livre apreciação da prova encontra-se previsto no artigo 127.º do Código de Processo Penal, dispondo o mesmo que, salvo as circunstâncias em que a lei dispuser em sentido contrário, a prova deverá ser apreciada de acordo com as regras da experiência e com a livre convicção da entidade para tal competente. Deste modo, é possível afirmar que a valoração da prova por parte do julgador encontra-se no âmbito da discricionariedade, mas uma discricionariedade que apresenta limites. Com efeito, ensina Jorge de Figueiredo Dias que "*Se a apreciação da prova é, na verdade, discricionária, tem evidentemente esta discricionariedade (...) os seus limites que não podem ser licitamente ultrapassados: a liberdade de apreciação da prova é, no fundo, uma liberdade de acordo com um dever – o dever de perseguir a chamada 'verdade material' –, de tal sorte que a apreciação há-de ser, em concreto recondutível a critérios objetivos e, portanto, em geral suscetível de motivação e de controlo (...).*"[54]. É nesta senda que surgem os sentidos positivo e negativo deste princípio: como sentido positivo, temos os referidos limites de

[52] Cfr. alíneas a), b) e g) do n.º 1 do artigo 61º do Código de Processo Penal:
"*1 - O arguido goza, em especial, em qualquer fase do processo e salvas as exceções da lei, dos direitos de:*
a) Estar presente aos atos processuais que diretamente lhe disserem respeito;
b) Ser ouvido pelo tribunal ou pelo juiz de instrução sempre que eles devam tomar qualquer decisão que pessoalmente o afete;
g) Intervir no inquérito e na instrução, oferecendo provas e requerendo as diligências que se lhe afigurarem necessárias;".
[53] Vide acórdão n.º 5/2010, de 06 de Janeiro, disponível em https://bityli.com/v7Oli, último acesso em 15-03-2022;
[54] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 203;

alcançar a realização da justiça e a descoberta da verdade material, numa apreciação motivada e, por isso, suscetível de controlo; já num sentido negativo, temos a ausência de critérios legais que operem uma pré-fixação relativamente ao valor a atribuir à prova[55].

Não obstante, existem várias exceções ao princípio da livre apreciação da prova, como sejam o valor da prova pericial, da confissão integral e sem reservas por parte do arguido, dos documentos autênticos e autenticados e, ainda, no que concerne ao pedido de indemnização cível, casos em que o juízo atinente aos mesmos se encontra subtraído à livre apreciação do julgador[56].

Igualmente relacionado com a matéria da prova, encontra-se o princípio da presunção de inocência, previsto, entre nós, no n.º 2 do artigo 32.º da Constituição da República Portuguesa[57], no qual se pode ler que "*Todo o arguido se presume inocente até ao trânsito em julgado da sentença de condenação, devendo ser julgado no mais curto prazo compatível com as garantias de defesa*.". De acordo com este princípio, toda e qualquer condenação judicial deverá ter por base uma atividade probatória, que compete à acusação, sendo esta totalmente necessária para fixar a responsabilidade penal do arguido, não incumbindo a este a tarefa de demonstração da sua inocência[58]. Consequentemente, tornam-se inadmissíveis quaisquer presunções de culpa, na medida em que, no âmbito do processo penal, o arguido tem o direito de ser considerado inocente, até que o contrário resulte de toda a prova produzia nos autos, mediante sentença judicial transitada em julgado; assim como qualquer aplicação por antecipação de penas, encapotadas de medidas de coação, com base num rótulo preconcebido de culpado[59] [60].

O princípio da presunção da inocência encontra o seu fundamento no respeito pela dignidade da pessoa humana, surgindo como manifestação do Estado de Direito e como base da legitimação do poder punitivo exercido pelo Estado. Conforme realça Ana Raquel Conceição, este princípio "*(...) não se trata apenas de uma regra de natureza probatória, (...) mas antes de uma verdadeira garantia de defesa deste que apesar de ser arguido num processo penal é uma pessoa*

---

[55] Neste sentido, vide aresto do Supremo Tribunal de Justiça, datado de 11-07-2007, relativo ao processo n.º 1611/07, disponível em https://bityli.com/jwt9J, último acesso em 15-03-2022, no sumário do qual se pode ler que "*I - O princípio da livre apreciação da prova é um princípio atinente à prova, que determina que esta é apreciada, não de acordo com regras legais pré-estabelecidas, mas sim segundo as regras da experiência comum e de acordo com a livre convicção do juiz, uma livre convicção que não pode ser arbitrária ou subjetiva e, por isso, deve ser motivada. A motivação da convicção apresenta-se, pois, como o meio de controlo da decisão de facto, em ordem a garantir a objetividade e a genuinidade da convicção formada pelo tribunal.*";

[56] A este respeito, vide artigos 163.º n.º 1, 344.º, 169.º e 84.º, todos do Código de Processo Penal.

[57] Num plano supranacional, vide artigos 11.º n.º 1 da Declaração Universal dos Direitos do Homem e 6.º n.º 2 da Convenção Europeia dos Direitos do Homem;

[58] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume I, 4ª edição, Editorial Verbo, 2000, p. 303;

[59] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 58;

[60] Vide, neste sentido, acórdão do Supremo Tribunal de Justiça, datado de 09-02-2012, relativo ao processo n.º 1/09.3FAHRT.L1.S1, disponível em https://bityli.com/OYgK9, último acesso em 15-03-2022, no qual se pode ler que "*A presunção de inocência incorpora um comando dirigido ao julgador no sentido de impor que as normas penais não consagrem presunções de culpa relativamente ao arguido e nem um ónus de prova a seu cargo para ser absolvido , beneficiando de um estado de dúvida razoável instalado no processo, além de dever ser tratado como autêntico sujeito processual e não como mero objeto , um simples contraditor , em igualdade de armas.*";

e merece sempre, a proteção da sua dignidade enquanto tal."[61]. Previsto no n.º 2 do artigo 6.º da Convenção Europeia dos Direitos do Homem[62], o princípio da presunção da inocência não abrange apenas o processo penal, mas antes apresenta uma aplicação transversal a processos de outras naturezas. Tal circunstância ficou patente no acórdão proferido pelo Tribunal Europeu dos Direitos do Homem, no âmbito do processo Melo Tadeu v. Portugal, onde o Estado Português foi condenado por violação do princípio da presunção da inocência, pelo facto de os tribunais administrativos terem condenado Maria Fernanda de Melo Tadeu com fundamento na sua culpa, apesar de a mesma já ter sido absolvida, de forma definitiva, pelos tribunais criminais[63].

Sintetizando todas as consequências que advêm do princípio da presunção de inocência, Gomes Canotilho e Vital Moreira entendem fazer parte do conteúdo deste princípio as seguintes: "*(a) proibição de inversão do ónus da prova em detrimento do arguido; (b) preferência pela sentença de absolvição contra o arquivamento do processo; (c) exclusão da fixação de culpa em despachos de arquivamento; (d) não incidência de custas sobre arguido não condenado; (e) proibição de antecipação de verdadeiras penas a título de medidas cautelares; (f) proibição de efeitos automáticos da instauração do procedimento criminal; (g) natureza excecional e de última instância das medidas de coação, sobretudo as limitativas e proibitivas da liberdade; (h) princípio in dubio pro reo, implicando a absolvição em caso de dúvida do julgador sobre a culpabilidade do acusado*."[64].

Por último, cumpre atentar no princípio *in dubio pro reo*, decorrente do princípio *supra* analisado, que postula que a incerteza dos factos, decorrente da deficitária produção de prova ocorrida em todo o processo, determina uma decisão favorável ao arguido. O mesmo é dizer que a falta de prova, em processo penal, tem o mesmo valor que a incerteza ou insuficiência da mesma, implicando como consequência última a impossibilidade de prossecução do processo contra o arguido e, bem assim, a sua absolvição[65]. Valendo para toda a matéria de facto, mas já não no que concerne à matéria de Direito, este princípio estipula que um *non liquet* relativo à prova terá sempre de ser valorado de modo favorável ao arguido[66]. A dúvida razoável reverterá, assim, sempre, a favor do arguido.

---

[61] CONCEIÇÃO, Ana Raquel, "Presunção da Inocência", In: Paulo Pinto de Albuquerque (Org.), *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, Volume II, Lisboa, Universidade Católica Editora, 2019, p. 1076;

[62] Vide artigo 6.º n.º 2 da Convenção Europeia dos Direitos do Homem:
"*2. Qualquer pessoa acusada de uma infração presume-se inocente enquanto a sua culpabilidade não tiver sido legalmente provada.*".

[63] Vide acórdão do Tribunal Europeu dos Direitos do Homem, datado de 23 de Dezembro, relativo ao processo n.º 27785/10, caso Melo de Tadeu v. Portugal, disponível em https://bityli.com/9Kvql, último acesso em 17-08-2021;

[64] CANOTILHO, J. Gomes, e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume I, 4ª edição, Coimbra Editora, 2007, p. 518.

[65] FERREIRA, Manuel Cavaleiro de, *Curso de Processo Penal*, Volumes I e II, Lisboa, Lições proferidas no ano letivo 1954-1955, pp. 310-311;

[66] DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004, p. 213.

Os princípios *supra* mencionados e analisados devem ser aplicados e observados em todos os atos que, de uma ou outra forma, dizem respeito à prova e à sua produção, nomeadamente aos meios de prova e meios de obtenção de prova, dos quais se tratará *infra*.

1.3. Meios de prova e meios de obtenção de prova

O Livro III do Código de Processo Penal dedica-se, na sua totalidade, à matéria da prova no âmbito do processo penal, indicando, entre outras disposições, quais os diferentes meios de prova e meios de obtenção de prova previstos na lei, pelo que interessa proceder à respetiva distinção.

De acordo com a definição avançada por Manuel Simas Santos, João Simas Santos e Manuel Leal Henriques, os meios de prova traduzem-se nos "*(...) veículos ou caminhos através dos quais se desenvolve a atividade probatória destinada à demonstração dos factos relevantes atinentes ao crime que se quer investigar*."[67]. Desta forma, uma vez trazidos a juízo os factos alegados pelas partes, deverá proceder-se à demonstração da realidade dos mesmos, mediante a utilização de elementos de que o julgador se serve para formar a sua convicção.

Conforme já *supra* mencionado, no que respeita à previsão normativa dos meios de prova, vigora o princípio da admissibilidade e liberdade de qualquer meio de prova, porquanto, de acordo com o artigo 125.º do Código de Processo Penal, são admissíveis todos os meios de prova, desde que não sejam proibidos por lei. Tal implica que o Código de Processo Penal não proceda, nos seus artigos 128.º a 170.º, a uma enumeração taxativa dos meios de prova ao dispor dos agentes processuais.

Não obstante esta inexistência de um *numerus clausus* de meios de prova, surge a questão de compreender em que medida seria possível modificar o regime legal de determinado meio de prova, excluindo apenas algumas das suas regras, estando, assim, perante um meio de prova atípico. No que se reporta a esta problemática, subscrevemos a opinião formulada por Germano Marques da Silva, de acordo com a mesma tal não será, de todo, possível. Nesta senda, justifica o autor que "*Com efeito, parece que a não tipicidade dos meios de prova que o art. 125.º estabelece respeita apenas a meios de prova não previstos e a não tipicidade dos meios não pode significar liberdade relativamente aos meios já disciplinados*."[68]. Parece-nos que, de facto, não faria sentido o legislador preocupar-se com a previsão normativa exaustiva relativamente a um certo

[67] SANTOS, Manuel Simas, SANTOS, João Simas, e LEAL-HENRIQUES, Manuel, *Noções de Processo Penal*, 2ª Edição, Lisboa, Rei dos Livros, 2011, p. 198.
[68] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, p. 160;

meio de prova para, posteriormente, admitir que, no seio do processo penal, se operassem alterações que, em última *ratio*, acabariam por desvirtualizar o modelo criado.

No Código de Processo Penal, encontram-se previstos como meios de prova, que de seguida iremos tratar, a prova testemunhal (artigos 128.º a 139.º), as declarações de arguido, assistente e partes civis (artigos 140.º a 145.º), a prova por acareação (artigo 146.º), a prova por reconhecimento (artigos 147.º a 149.º), a prova por reconstituição do facto (artigo 150.º), a prova pericial (artigos 151.º a 163.º) e a prova documental (artigos 164.º a 170.º).

A prova testemunhal, regulamentada nos artigos 128.º a 139.º do Código de Processo Penal, tem por objeto os factos de que a testemunha tem conhecimento direto e que, ao mesmo tempo, constituem objeto de prova. Assim, o que releva para efeitos de prova será o conhecimento direto da testemunha, sendo que, se do depoimento da mesma resultar que o seu conhecimento apenas advém do que ouviu terceiros a dizer, o mesmo não poderá servir como meio de prova, no que a essa parte diz respeito, nos termos do disposto no n.º 1 do artigo 129.º do Código de Processo Penal. No seu depoimento, está a testemunha obrigada a responder com verdade às questões que lhe forem colocadas, sob pena de, se não o fizer, incorrer em responsabilidade criminal, mormente no crime de falsidade de testemunho, de acordo com o disposto nos artigos 132.º n.º 1 d) do Código de Processo Penal e 360.º do Código Penal. Apenas assim não será se das suas respostas resultar a sua responsabilização penal, caso em que a testemunha se pode recusar a responder às perguntas formuladas, conforme prevê o n.º 2 do artigo 132.º do Código de Processo Penal.

Tendo em conta o caráter pessoal deste meio de prova, Fernando Gonçalves e Manuel Alves alertam para a margem de erro ao mesmo associada, na medida em que "*Na maioria dos processos, a prova testemunhal é o único meio de prova ou, pelo menos, o principal, o que obriga a uma grande atenção para os riscos de falibilidade que este meio de prova encerra. É conhecida a fragilidade humana perante determinadas circunstâncias, em que, tantas vezes, os interesses pessoais e materiais, se sobrepõem, aos valores e princípios da justiça e da verdade*."[69].

Por seu turno, as declarações de arguido, assistente e partes civis encontram-se previstas nos artigos 140.º a 145.º do Código de Processo Penal. Ao contrário do que sucede com as declarações do assistente e das partes civis, que se traduzem num meio de prova, equiparado à prova testemunhal, as declarações do arguido caracterizam-se como sendo, simultaneamente, um meio de prova e um meio de defesa ao dispor do mesmo. Perante as questões colocadas acerca

[69] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, pp. 151-152.

dos factos em discussão nos autos, o arguido pode adotar um de três diferentes comportamentos, a saber: negar todos os factos que lhe são imputados; confessar os factos que lhe são imputados; ou remeter-se ao silêncio. Independentemente da opção que tomar, o arguido deverá estar sempre livre na sua pessoa, ainda que detido ou preso, e encontra-se adstrito a um dever de responder com verdade no que respeita às matérias relativas à sua identificação, sob pena de incorrer em responsabilidade penal, não devendo nunca prestar juramento[70].

Caso o arguido pretenda negar a imputação dos factos, não poderá ser responsabilizado se tal declaração se relevar falsa, uma vez que não cumpre ao arguido colaborar com a justiça para obter uma eventual condenação. Tal como refere Maria João Antunes, "*Não se trata aqui do reconhecimento de um direito à mentira, mas tão só de que é inexigível ao arguido o cumprimento do dever de verdade, não impendendo sobre ele qualquer dever de colaboração com a administração da justiça penal.*"[71]. Caso pretenda, por outro lado, confessar os factos que lhe são imputados, o tribunal deverá procurar avaliar o caráter livre de tal confissão e, caso entenda que assim seja, determinar as consequências previstas no n.º 2 do artigo 344.º do Código de Processo Penal. Por último, caso o arguido pretenda remeter-se ao silêncio, nos termos do disposto nos artigos 343.º n.º 1 e 345.º n.º 1 do Código de Processo Penal, não poderá esse silêncio desfavorecer o arguido, ser valorado como presunção de culpa ou, sequer, para determinação da medida da pena em caso de condenação. A única circunstância em que o silêncio do arguido se poderá tornar desfavorável é aquela em que o mesmo impossibilite o conhecimento, por parte do tribunal, de elementos de factos que teriam como finalidade atenuar uma sanção penal a aplicar.

O regime geral atinente às declarações do assistente e das partes civis encontra-se previsto no artigo 145.º do Código de Processo Penal, sendo, como já *supra* mencionado, equiparadas à prova testemunhal, com a exceção de que, tanto o assistente como as partes civis não devem prestar juramento, nos termos do n.º 4 do referido preceito legal. Não obstante esta dispensa de prestar juramento, os mesmos encontram-se adstritos ao dever de verdade, devendo as suas declarações ser requeridas pelos próprios, pelo arguido ou pela entidade judiciária, conforme resulta do n.º 1.

A acareação, prevista no artigo 146.º do Código de Processo Penal, traduz-se "*(...) no confronto entre as pessoas que prestaram declarações contraditórias, tendo por finalidade esclarecer depoimentos divergentes sobre o mesmo facto.*"[72]. Pode ocorrer entre quaisquer

[70] Cfr. artigos 140.º n.º 1 e 3, 141.º n.º 3, 61.º n.º 6 b), todos do Código de Processo Penal, e 360.º do Código Penal;
[71] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, p. 123.
[72] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, p. 210;

pessoas que prestem declarações no âmbito do processo penal, com a exceção dos peritos, tendo lugar oficiosamente ou a requerimento, conforme postula o n.º 1 do artigo 146.º do Código de Processo Penal. Como pressupostos deste meio de prova temos a existência de declarações anteriores contraditórias; a utilidade da diligência para a descoberta da verdade; e, ainda, o facto de as declarações contraditórias puderem ser utilizadas como meio de prova na fase em que se procede à acareação.

Por seu turno, a prova por reconhecimento revela-se como a confirmação, pela pessoa que procede ao ato, de uma pessoa ou objeto conhecido anteriormente, pelo que se trata, deste modo, de um meio de prova confirmador de um elemento de prova que já foi previamente admitido aos autos[73]. O reconhecimento de pessoas encontra-se previsto no artigo 147.º do Código de Processo Penal, ao passo que o reconhecimento de objetos se encontra previsto no artigo 148.º do referido diploma legal. Tanto o reconhecimento de pessoas, como o reconhecimento de objetos deve obedecer às regras previstas nestes artigos, sob pena de não terem valor de meio de prova, seja qual for a fase do processo em que ocorrer, de acordo com o disposto no n.º 7 do artigo 147.º do Código de Processo Penal. Anteriormente a ser inserida esta alteração no Código de Processo Penal, decidiu o Tribunal Constitucional ser "*(...) claramente lesivo do direito de defesa do arguido, consagrado no nº 1 do artigo 32º da Constituição, interpretar o artigo 127º do Código de Processo Penal no sentido de que o princípio da livre apreciação da prova permite valorar, em julgamento, um ato de reconhecimento realizado sem a observância de nenhuma das regras previstas no artigo 147º do mesmo diploma*."[74].

A prova por reconstituição do facto, prevista no artigo 150.º do Código de Processo Penal, traduz-se na reprodução, tão fidedigna quanto possível, das condições em que se afirma ou supõe ter ocorrido o facto e na repetição do modo de realização do mesmo. A surpresa e a falta de preparação são essenciais no que diz respeito a este meio de prova, por modo a evitar que sejam realizadas encenações prévias que teriam como consequência a facilidade de repetição perante o tribunal, afetando, assim, de forma clara a tarefa de descoberta da verdade. Nesta senda, dispõe o n.º 3 do *supra* mencionado preceito legal que a publicidade da diligência de prova deve, na medida do possível, ser evitada.

De acordo com o disposto no artigo 151.º do Código de Processo Penal, há lugar a prova pericial quando a apreciação dos factos exigir especiais conhecimentos técnicos, científicos e

[73] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 175;
[74] Vide acórdão n.º 137/01, de 28 de Março, relativo ao processo n.º 778/00, disponível em https://bityli.com/SoNwt, último acesso em 15-03-2022;

artísticos, razão pela qual o seu valor se presume subtraído à livre apreciação do julgador, conforme postula o artigo 163.º do referido diploma legal. No seio do nosso processo penal, não há lugar a uma contraditoriedade da perícia, na medida em que o perito nomeado é um perito do tribunal, com ausência de indicação de perito, quer por parte da acusação, quer por parte da defesa. Há, contudo, uma exceção, uma vez que o tribunal admite que o Ministério Público, arguido, assistente e partes civis possam designar consultores técnicos da sua confiança para assistir à perícia, conforme resulta dos artigos 152.º n.º 1 e 155.º n.º 1 do Código de Processo Penal.

Por último, a prova documental encontra-se regulamentada nos artigos 164.º a 170.º do Código de Processo Penal, nos termos dos quais os documentos devem ser juntos aos autos durante o inquérito ou a instrução, e, não sendo tal possível, até ao encerramento da audiência de discussão e julgamento. No que concerne ao seu valor probatório, são dados como provados os factos constantes dos documentos autênticos e autenticados, desde que a sua autenticidade e veracidade não seja colocada em causa, de forma fundamentada, tal como dispõe o artigo 169.º do Código de Processo Penal. Trata-se, assim, de uma exceção ao princípio da livre apreciação da prova por parte do julgador.

Distintos dos meios de prova, *supra* analisados, são os meios de obtenção de prova, tratando-se estes de "*(...) instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova; não são instrumentos de demonstração do thema probandi, são instrumentos para recolher no processo esses instrumentos*."[75]. Para Germano Marques da Silva, os meios de obtenção de prova distinguem-se dos meios de prova numa *dupla dimensão*: numa dimensão lógica, os meios de prova são, por si só, fonte de convencimento, ao passo que os meios de obtenção de prova apenas possibilitam a obtenção dos meios de prova; numa dimensão técnico-operativa, os meios de obtenção de prova caracterizam-se pelo modo e momento da sua aquisição no âmbito do processo penal[76]. Não obstante, em determinados casos, o próprio meio de obtenção de prova acaba por ser, igualmente, um meio de prova, tal como acontece, a título de exemplo, com as escutas telefónicas, que são um meio de obtenção de prova, mas as gravações já são um meio de prova. Como meios de obtenção de prova tipificados no Código de Processo Penal temos os exames, as revistas e buscas, as apreensões e as escutas telefónicas.

[75] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, p. 233;
[76] *Idem*, pp. 233-234.

Os exames, legalmente previstos nos artigos 171.º a 173.º do Código de Processo Penal, ocorrem com o intuito de inspecionar vestígios que o crime possa ter deixado, bem como todos os indícios relativamente ao modo e lugar como e onde foi o mesmo praticado, as pessoas que o cometeram e sobre quem foi cometido. Podem ter lugar por iniciativa dos órgãos de polícia criminal, contudo, é da competência reservada do juiz o exame que envolva as características físicas e psíquicas de uma pessoa que não tenha prestado o seu consentimento para tal ato, nos termos do n.º 2 do artigo 172.º do Código de Processo Penal. Este meio de obtenção de prova pode ter lugar ainda antes de se ter iniciado o procedimento criminal, como uma providência cautelar quanto aos meios de prova, conforme regula o artigo 249.º do Código de Processo Penal, e distingue-se das perícias, na medida em que na perícia existe uma exigência de especiais conhecimentos técnicos, científicos e artísticos, enquanto que nos exames se inspeciona os vestígios mas tal inspeção não só não exige os referidos conhecimentos, como tais vestígios serão objeto de perícia ou livremente valorados pela autoridade judiciária competente.

As revistas e as buscas encontram-se regulamentadas nos artigos 174.º a 177.º do Código de Processo Penal e diferem quanto ao seu objeto. As revistas têm por objeto as pessoas e ocorrem quando existirem indícios de que alguém oculta, na sua pessoa, quaisquer objetos relacionados com a prática de um crime ou que possam servir de prova. As buscas têm por objeto os locais, sendo ordenadas quando existirem indícios de que, em lugar reservado ou não livremente acessível ao público, se encontrem objetos relacionados com o crime ou que possam servir de prova, com o arguido ou pessoa que deva ser detida. Tanto as revistas como as buscas são ordenadas por despacho da autoridade judiciária competente, com exceção dos casos previstos no n.º 5 do artigo 174.º do Código de Processo Penal. Cumpre apenas destacar que, no que toca às buscas domiciliárias, as mesmas apenas podem ser ordenadas pelo juiz, de acordo com os artigos 177.º nº. 1 e 269.º n.º 1 alínea c) do Código de Processo Penal, com exceção do disposto no n.º 3 do artigo 177.º do referido diploma legal, casos em que pode ser ordenada pelo Ministério Público. A busca a escritório de advogado ou consultório médico é necessariamente presidida pelo juiz, conforme estipula o n.º 5 do artigo 177.º.

As apreensões, previstas nos artigos 178.º a 186.º do Código de Processo Penal, incidem sobre instrumentos, produtos ou vantagens relacionadas com a prática de um crime, bem como os objetos deixados no local do crime pelo agente. São ordenadas e validadas por despacho da autoridade judiciária competente, podendo igualmente ser efetuadas pelos órgãos de polícia criminal, nos termos dos n.º 3, 4, 5 e 6 do artigo 178.º do Código de Processo Penal. A apreensão

de correspondência dispõe de um regime distinto, previsto no artigo 179.º do *supra* mencionado diploma legal.

Por seu turno, as escutas telefónicas encontram-se previstas nos artigos 187.º a 190.º do Código de Processo Penal, apenas podendo ser autorizadas por despacho fundamentado do juiz de instrução, a requerimento do Ministério Público. Tendo em conta a excecionalidade deste meio de obtenção de prova, refere Maria João Antunes que "*A natureza marcadamente subsidiária e excecional deste meio de obtenção de prova, subordinado aos denominados 'crimes de catálogo', a competência reservada do juiz de instrução e a cominação de nulidade em caso de inobservância dos seus requisitos e condições revelam a intenção de harmonizar a finalidade de realização da justiça e descoberta da verdade material com a proteção dos direitos fundamentais sacrificados na escuta telefónica.*"[77].

Para finalizar, cumpre apenas salientar que existem outros meios de obtenção de prova não previstos no Código de Processo Penal, mas sim em legislação avulsa, como é o caso das ações encobertas, alvo do presente estudo e previstas na Lei n.º 101/2001, de 25 de Agosto, às quais será dado o devido tratamento nos seguintes capítulos.

1.4. Proibições de prova e o efeito à distância da prova proibida

A problemática das proibições de prova assume um papel central no Direito Processual Penal, dada a sua elevada complexidade e o impacto que tem nos direitos fundamentais que assistem aos cidadãos.

A expressão *proibições de prova* foi pela primeira vez utilizada pelo jurista alemão Ernst von Beling, no ano de 1902, pretendendo com a mesma aludir para a existência de limites à descoberta da verdade material no âmbito do processo penal, limites estes impostos pelo próprio Estado com o intuito de respeitar e proteger os direitos fundamentais dos indivíduos e, ainda, de salvaguardar determinados interesses públicos[78]. Posteriormente, nos Estados Unidos da América, a prolação do acórdão *Mapp* v. *Ohio*[79], em 1961, veio operar uma total revolução processual, porquanto decidiu que, as proibições de prova consequentes de atos violadores de direitos fundamentais consagrados na sua Constituição, se aplicariam de igual modo aos processos a

[77] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016, p. 118;
[78] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 177;
[79] Disponível em https://bityli.com/YoEMM, último acesso em 15-03-2022.

correr termos nos tribunais estaduais, ao invés do que até aí acontecia, em que só eram aplicadas nos processos atribuídos ao tribunais federais[80].

Foram, assim, a doutrina alemã e a jurisprudência norte-americana que contribuíram para um primeiro desenho do sistema alusivo às proibições de prova, sendo que as primeiras proibições de prova começaram por ser apenas relativas aos atos de produção de prova ocorridos em sede de audiência de discussão e julgamento, e só depois se estenderam aos atos anteriores à referida audiência, isto é, a atos de investigação criminal anteriores à acusação. Esta abrangência aos atos de investigação surge por força do princípio da não autoincriminação, uma vez que era frequente existirem, na fase de investigação, confissões obtidas de forma indevida e abusiva[81].

No que ao aparecimento desta problemática no Direito português diz respeito, Paulo Dá Mesquita refere que "*Nos diversos processos penais existem, há muito, instrumentos jurídicos condicionadores de acesso à informação e que determinam a exclusão ou inatendibilidade de dados indevidamente obtidos. A consagração das proibições de prova constitucionais, contudo, relaciona-se com uma linha marcante desenvolvida pela jurisprudência do Supremo Tribunal dos Estados Unidos, em que se extrai da Constituição, para além do fim central da regulação da descoberta da verdade no respeito de direitos fundamentais, um novo patamar de afastamento da prova por força da violação de imperativos constitucionais na sua obtenção.*"[82].

Fortemente influenciados por esta jurisprudência norte-americana, os autores portugueses foram tentando definir esta expressão *proibições de prova*. Para Germano Marques da Silva, com as proibições de prova tem-se como objetivo tentar evitar que sejam sacrificados direitos fundamentais dos cidadãos por parte das autoridades judiciárias, tendo como consequência a privação de eficácia das provas obtidas ou produzidas de modo ilegal. Para este autor, caso a obtenção de meios de prova resulte na violação de direitos dos cidadãos, as provas obtidas através de tal violação não podem ser atendidas no âmbito do processo penal[83]. Por seu turno, no entendimento do juiz de Direito João de Martos-Cruz Praia, as proibições de prova significam, de forma muito simples, algo de que o tribunal não se pode servir para formar a sua convicção ou fundamentar a sua decisão[84].

---

[80] MESQUITA, Paulo Dá, *A Prova do Crime e O Que Se Disse Antes do Julgamento: Estudo sobre a Prova no Processo Penal Português, à Luz do Sistema Norte-Americano*, Coimbra Editora, 2011, pp. 209-210.
[81] *Idem*, pp. 214-215;
[82] *Idem*, p. 270;
[83] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, p. 138;
[84] PRAIA, João de Matos-Cruz, "Proibições de prova em processo penal: algumas particularidades no âmbito da prova por reconhecimento e da reconstituição do facto", in *Julgar Online*, Dezembro de 2019, p. 3, disponível em https://bityli.com/2qWxq.

Essencial para um melhor entendimento da problemática das proibições de prova foi o trabalho desenvolvido por Manuel da Costa Andrade, de acordo com o qual estas são "*(...) barreiras colocadas à determinação dos factos que constituem objeto do processo*.", sendo essencial neste conceito a "*(...) prescrição de um limite à descoberta da verdade material*."[85]. Nesta senda, as proibições de prova distinguem-se das regras de produção de prova, na medida em que estas últimas têm apenas como objetivo disciplinar o procedimento de produção da prova, nos seus diferentes meios e métodos de obtenção, não cabendo a estas determinar uma qualquer violação ou proibição de valoração. Não se tratando de limites à prova, como sucede com as proibições de prova, as regras de produção de prova disciplinam os modos como a produção de prova deve ser levada a cabo. Entende o autor que "*Umas vezes preordenadas à maximização da verdade material (...), as regras de produção da prova podem igualmente ser ditadas para obviar ao sacrifício desnecessário e desproporcionado de determinados bens jurídicos*."[86].

Atualmente, a doutrina dominante procede a uma divisão das proibições de prova em proibições de produção de prova e proibições de valoração de prova, pelo que iremos, de seguida, atentar nas especificidades e consequências de cada uma.

No que respeita às proibições de produção de prova, as mesmas podem consubstanciar-se em temas de prova proibidos, meios de prova proibidos ou, ainda, métodos de prova proibidos.

Os temas de prova proibidos traduzem-se naqueles em que a lei não permite que se proceda à sua investigação, como é o caso do disposto nos artigos 137.º e 182.º do Código de Processo Penal, no âmbito dos quais a salvaguarda do segredo de Estado tem prevalência sobre a descoberta da verdade material. Nos termos dos referidos preceitos legais, se determinada autoridade judiciária inquirir uma testemunha acerca de factos que constituam segredo de Estado, sem que a mesmo se tenha escusado, quando o deveria ter feito, o seu depoimento não poderá ser valorado no processo penal.

Por seu turno, os meios de prova proibidos são "*(...) aqueles que a lei não permite que se valorizem como meio de prova por lhes faltar um qualquer requisito legal (...)*"[87], sendo exemplos dos mesmos o caso das testemunhas não esclarecidas acerca da faculdade de recusa de depoimento, previsto no n.º 2 do artigo 134.º do Código de Processo Penal, das declarações de coarguido em prejuízo de outro coarguido, quando aquele se recusar a responder às questões colocadas sobre os factos que lhe são imputados, previsto no nº. 4 do artigo 345.º do Código de

[85] ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, 1992, p. 83.
[86] *Idem*, pp. 84-85;
[87] JESUS, Francisco Marcolino de, *Os Meios de Obtenção da Prova em Processo Penal*, Almedina, 2011, p. 82.

Processo Penal, e da leitura proibida de autos e declarações, previsto no n.º 6 do artigo 356.º do Código de Processo Penal.

Já os métodos de prova proibidos dizem respeito aos procedimentos utilizados pelas autoridades judiciárias, órgãos de polícia criminal e partes no processo para obtenção de meios de prova, mediante condutas contrárias aos direitos dos cidadãos, mormente de liberdade, salvo exceções expressamente previstas na Constituição da República Portuguesa[88]. De acordo com Manuel da Costa Andrade, "*A coberto dos métodos proibidos de prova prescreve a lei processual os atentados mais drásticos à dignidade humana, mais capazes de comprometer a identidade e a representação do processo penal como processo de um Estado de Direito e, por vias disso, abalar os fundamentos daquela Rechtskultur sobre que assenta a moderna consciência democrática*."[89].

Sob a epígrafe *Garantias de processo criminal*, o artigo 32.º da Constituição da República Portuguesa, no seu n.º 8, prevê que 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, são consideradas nulas. Sendo o Direito Processo Penal considerado, como já *supra* aludido, direito constitucional aplicado, a Constituição da República Portuguesa determinou que a concordância das provas obtidas com a dignidade da pessoa humana merece acolhimento na temática dos direitos fundamentais[90]. Da análise do referido preceito legal e do disposto nos n.º 2, 3 e 4 do artigo 34.º do mesmo diploma, é possível observar que são considerados como métodos absolutamente proibidos a tortura, a coação e a ofensa à integridade física e moral da pessoa, e como métodos relativamente proibidos a intromissão abusiva na vida privada, no domicílio, correspondência e telecomunicações da pessoa, porquanto estes últimos podem vir a ter lugar nos casos expressamente previstos na lei ou mediante acordo da pessoa visada, afastando, assim, a proibição.

O artigo 126.º do Código de Processo Penal determina, de igual modo, os métodos de prova proibidos, que atentam contra a liberdade e violam a dignidade das pessoas pelos mesmos visadas, sendo igualmente proibidos por este preceito legal os métodos já indicados no n.º 8 do artigo 32.º da Constituição da República Portuguesa. Os métodos de prova proibidos apresentam como sujeitos passivos o arguido, as testemunhas e os peritos. No que respeita ao arguido, tal decorre do seu estatuto como sujeito processual; já no que concerne às testemunhas e aos peritos,

[88] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 179.
[89] ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, 1992, p. 209;
[90] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 179.

aos mesmos deve, de igual modo, ser dado o devido respeito pela sua dignidade, contudo, não se pode olvidar que os mesmos estão obrigados a depor e adstritos ao dever de verdade[91].

Cumpre, ainda, esclarecer que o artigo 126.º do Código de Processo Penal não se traduz numa enumeração taxativa dos métodos de prova proibidos existentes, devendo, igualmente, "*(...) valorar-se os demais atentados à dignidade humana, à liberdade de decisão ou de vontade ou à integridade física ou moral das pessoas.*"[92]. Não obstante, apesar de ser clara a conclusão de que não são permitidas as provas decorrentes dos métodos previstos no preceito legal vindo de referir, tal já não sucede quando questionamos a possibilidade de utilização de métodos não previstos, como seja o polígrafo ou detetor de mentiras. Sem prejuízo do que acontece em ordenamentos jurídicos diferentes, em Portugal, a submissão de um arguido ao teste do polígrafo, contra a sua vontade, é expressamente proibida, sendo, todavia, discutida a sua admissibilidade, caso o arguido preste o devido consentimento. Na tese defendida por Manuel da Costa Andrade, apesar de entender que o polígrafo não deve ser utilizado como instrumento ao dispor da acusação, não existem razões para ditar a sua proibição relativamente à defesa. Com efeito, para o autor "*A sua utilização pode mesmo revelar-se aconselhável naqueles casos extremados em que apareça como a ultima ratio para afastar uma condenação.*"[93].

Ora, não podemos concordar com a opinião formulada pelo Autor, na medida em que o teste do polígrafo regista alterações e variações fisiológicas no decurso do interrogatório, considerando que o arguido se encontra a mentir quando tais variações se afastam dos padrões considerados normais. Ainda que usado numa ótica de defesa, podem ocorrer variações fisiológicas da mais variada natureza, sem que tal signifique que o arguido está a mentir. O que inicialmente se pretendia que resultasse em favor do arguido e evitasse uma condenação pode, na verdade, ter um efeito oposto, tudo com base em métodos extremamente duvidosos e não comprovados cientificamente.

As proibições de valoração de prova, distintas das proibições de produção de prova, "*(...) emergem e relevam assim do conflito de interesses individuais e o interesse de perseguição penal. Só pode afirmar-se a sua existência quando a consideração da concreta situação de conflito faz aparecer a prevalência do interesse individual, porque o princípio do Estado de Direito reclama a garantia e efetivação do bem jurídico individual face à atividade de perseguição do Estado.*"[94]. A violação das proibições de produção de prova terá como consequência, em princípio, a

[91] ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, 1992, pp. 212-213;
[92] *Idem*, p. 216;
[93] *Idem*, pp. 218-219.
[94] *Idem*, p. 33;

impossibilidade de valoração das mesmas. Todavia, pode acontecer que a violação das proibições de produção de prova não tenha qualquer tipo de consequência, como é o caso dos exames e revistas que possam atentar contra o pudor dos visados. Aqui, apesar de o disposto nos artigos 172.º n.º 2 e 175.º n.º 2 do Código de Processo Penal dever ser respeitado, na hipótese de não o ser, tal não vai impedir a valoração das provas que daí advêm[95].

Numa hipótese contrária, poderemos, ainda, estar perante uma produção de valoração de prova independente, isto é, totalmente alheia à existência de vícios na etapa anterior de produção de prova. Trata-se de casos em que, mesmo não existindo uma qualquer violação de proibições de produção de prova, a mesma não poderá ser valorada no processo penal[96]. Como exemplo, temos o caso das escutas telefónicas devidamente autorizadas e legais que gravam conversas que excedem o objeto do processo em curso, os denominados conhecimentos fortuitos, ou seja, independentes do crime cuja investigação legitimou a escuta telefónica. Nestas situações, as conversas gravadas apenas poderão ser valoradas se pertencerem ao catálogo de crimes previsto no artigo 187.º do Código de Processo Penal.

Cumpre, ainda, esclarecer o que sucede, no âmbito do processo penal, quando ocorrem efetivamente proibições de produção de prova. Nesta senda, várias têm sido as teses avançadas pela doutrina, entre si dissidentes, relativamente à relação das proibições de prova com o regime das nulidades processuais, previsto nos artigos 118.º a 123.º do Código de Processo Penal.

No entendimento de Germano Marques da Silva, as proibições de prova e o regime das nulidades são realidades distintas e autónomas, não obstante a utilização de uma prova proibida tenha como consequência os efeitos da nulidade do ato. Para o autor, apesar de a prova proibida ser nula e não poder ser utilizada no processo ou servir para fundamentar qualquer decisão, o regime das proibições de prova não há de reconduzir-se ao regime das nulidades processuais. A nulidade consequente da produção de prova proibida será de conhecimento oficioso até ao proferimento da decisão final, momento a partir do qual a mesma poderá ser invocada mas, desta feita, como fundamento de recurso extraordinário de revisão, nos termos do disposto na alínea e) do n.º 1 do artigo 449.º do Código de Processo Penal[97].

De forma distinta, Paulo de Sousa Mendes defende que o título V do livro II do Código de Processo Penal, relativo às nulidades processuais, não esgota todas as espécies de nulidades. Segundo o autor, o n.º 3 do artigo 118.º do Código de Processo Penal parece abrir portas à

[95] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 184;
[96] PRAIA, João de Matos-Cruz, "Proibições de prova em processo penal: algumas particularidades no âmbito da prova por reconhecimento e da reconstituição do facto", in *Julgar Online*, Dezembro de 2019, p. 12, disponível em https://bityli.com/2qWxq.
[97] SILVA, Germano Marques da, *Curso de Processo Penal*, Volume II, 4ª edição, Editorial Verbo, 2008, pp. 144-145;

possibilidade de existir um ou mais regimes *sui generis* para as nulidades resultantes de violação das normas enformadoras de proibições de prova, entendendo mesmo que tal foi o que aconteceu com o artigo 126.º do Código de Processo Penal, porquanto não se trata da previsão de uma nulidade em sentido técnico-processual, mas sim "*(...) uma 'nulidade' dotada de uma autonomia técnica completa em face do regime das nulidades processuais*."[98].

No nosso entender, parece-nos, de facto, que, ao individualizar a temática das proibições de prova no n.º 3 do artigo 118.º do Código de Processo Penal, pretendeu o legislador diferenciar as proibições de prova do regime das nulidades processuais, pelo que não devem os mesmos ser confundidos.

Sendo o resultado da violação de proibições de produção de prova a nulidade da prova que de daí adveio, resta saber o que acontece às provas seguintes, isto é, se a proibição e a nulidade valem só para a prova obtida diretamente através de uma proibição de prova ou se valem igualmente para as provas obtidas indiretamente da prova proibida. No que a esta questão diz respeito, surgiu nos Estados Unidos da América a denominada *Fruit of The Poisonous Tree Doctrine* (teoria dos frutos da árvore envenenada), e na Alemanha a correspondente *Makel-Theorie* (teoria da mácula), de acordo com as quais a proibição de prova inicial estende-se às provas obtidas indiretamente, ou seja, "*(...) arrastam um efeito-à-distância que consiste em tornarem inaproveitáveis as provas secundárias a elas causalmente vinculadas*."[99]. Como afloramento desta teoria temos o n.º 1 do artigo 122.º do Código de Processo Penal, de acordo com o qual "*As nulidades tornam inválido o ato em que se verificarem, bem como os que dele dependerem e aquelas puderem afetar*.", prevendo, assim, uma transmissão do vício resultante da nulidade inicial para os factos subsequentes que resultem da mesma. Um outro entendimento não se pode conceder, porquanto a não consagração deste efeito-à-distância levaria quase a um incentivo à utilização de métodos proibidos de prova, o que se traduziria, em *ultima ratio*, numa deficitária tutela dos direitos fundamentais dos cidadãos.

Como critérios aferidores da existência de efeito-à-distância, torna-se necessário recorrer às teorias da imputação objetiva em Direito Penal, como sejam a teoria da causalidade adequada, a esfera de proteção das normas, os processos hipotéticos e a causa virtual. Não obstante, os diferentes autores não parecem unânimes quanto à suficiência da existência de um nexo de imputação objetiva para estarmos perante um efeito-à-distância. Ao passo que Figueiredo Dias

[98] MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p. 187.
[99] *Idem*, p. 191.

parece entender que o pressuposto verificador do efeito-à-distância é a proteção da dignidade da pessoa humana, Costa Andrade defende a existência de dois pressupostos distintos, a saber: o fim de proteção da norma, de acordo com o qual é necessário averiguar se o que se pretende proteger com o estabelecimento da proibição são direitos fundamentais, caso em que se verificará um efeito-à-distância; e os processos hipotéticos de investigação, na senda dos quais se afasta o efeito-à-distância quando a prova mediata obtida poderia tê-lo sido mediante um meio lícito. Ainda que não haja um verdadeiro consenso, a base de todos os diferentes entendimentos doutrinários parece ser a mesma – o respeito pelos direitos fundamentais dos indivíduos e que tal esteja na base do estabelecimento da proibição de prova[100].

Independentemente do *supra* exposto, a doutrina dos frutos da árvore envenenada apresenta três exceções que, uma vez verificadas, têm como consequência a valoração da prova obtida indiretamente de uma proibição de prova, a saber: a fonte independente, a descoberta inevitável e a nódoa dissipada.

A fonte independente respeita a "*(...) um recurso probatório destacado do inválido, usualmente com recurso a meio de prova anterior que permite induzir, probatoriamente, aquele a que o originário tendia, mas que foi impedido, ou seja, quando a ilegalidade não foi conditio sine qua non da descoberta da verdade.*"[101]. Assim, esta exceção aceita as provas que poderiam ter sido obtidas de modo autónomo e lícito. Já a descoberta inevitável reporta-se à aceitação das provas que, independentemente da proibição inicial, iam acabar por ser descobertas, de forma inevitável, ainda que num momento posterior e através de outro método de investigação criminal. Por seu turno, a nódoa dissipada relaciona-se com a aceitação de uma prova que, mesmo proveniente de uma proibição de prova, apresente uma autonomia suficiente de tal ordem que atenua a ilegalidade originária, dissipando a nódoa.

No ordenamento jurídico português foi particularmente relevante nesta matéria o Acórdão do Tribunal Constitucional, com o n.º 198/2004, no âmbito do qual foi confirmada a total aplicação, entre nós, da doutrina do efeito-à-distância, tendo, contudo, no caso em apreço considerado o Tribunal que a ilegalidade da prova originária não afetava uma posterior confissão voluntária e esclarecida, uma vez que tal se traduz num ato independente, praticado com livre vontade[102].

---

[100] CONCEIÇÃO, Ana Raquel, *Escutas Telefónicas – Regime Processual Penal*, Lisboa, Quid Iuris, 2009, pp. 199-200;

[101] GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009, p. 139.

[102] Vide, neste sentido, Acórdão n.º 198/2004, de 24 de Março, relativo ao processo n.º 39/04, disponível em https://bityli.com/9p0OT, último acesso em 15-03-2022, no qual se pode ler que: "*(...) está em causa a norma do artigo 122º nº 1 do CPP, entendida como autorizando, face à nulidade/invalidade de interceções telefónicas realizadas, a utilização de outras provas, distintas das escutas e a elas subsequentes, quando tais provas se traduzam nas declarações dos próprios arguidos, designadamente quando tais declarações sejam confessórias. Pode, assim, afirmar-se*

Uma vez analisada a matéria atinente à prova e a todas as suas especificidades, iremos de seguida abordar a temática das ações encobertas, procurando compreender melhor como estas se desenrolam, qual a sua base legal e, ainda, a forma como as mesmas são tratadas noutros ordenamentos jurídicos.

com segurança que o sentido de uma norma prescrevendo que a invalidade do ato nulo se estende aos que deste dependerem ou que ele possa afetar (artigo 122º, nº 1 do CPP) é, desde logo, o de abrir caminho à ponderação que – como adiante se verá - subjaz à chamada doutrina dos «frutos proibidos». Isto, cotejado com a apontada amplitude das garantias de defesa contidas no artigo 32º da CRP, leva a que este Tribunal considere que, efetivamente, certas situações de «efeito-à-distância» não deixam de constituir uma das dimensões garantísticas do processo criminal, permitindo verificar se o nexo naturalístico que, caso a caso, se considere existir entre a prova inválida e a prova posterior é, também ele, um nexo de antijuridicidade que fundamente o «efeito-à-distância», ou se, pelo contrário, existe na prova subsequente um tal grau de autonomia relativamente à primeira que a destaque substancialmente daquela. (...) o entendimento do artigo 122º, nº 1 do CPP, subjacente à decisão recorrida, segundo o qual este abre a possibilidade de ponderação do sentido das provas subsequentes, não declarando a invalidade destas, quando estiverem em causa declarações de natureza confessória, mostra-se constitucionalmente conforme, não comportando qualquer sobreposição interpretativa a essa norma que comporte ofensa ao disposto nos preceitos constitucionais invocados.".

2. AS AÇÕES ENCOBERTAS

Ao longo dos últimos anos temos assistido a um aumento e evolução galopantes, não só da criminalidade organizada, como também dos meios de que esta se serve para se introduzir no seio de determinada sociedade. Tal evolução aliada à ameaça permanente do terrorismo, ao constante processo de globalização e, ainda, ao surgimento de tecnologias cada vez mais sofisticadas, tem como consequência o incremento exponencial da prática de factos ilícitos e a redução de possibilidade de deteção e punição dos mesmos[103]. Tendo como objetivo imediato, a procura pelo lucro rápido e como objetivo mediato o controlo total do poder político social e económico, a criminalidade organizada necessita de uma rede bem estabelecida para se inserir e enraizar e aproveita todas as lacunas legais que possa encontrar para ganhar progressivamente mais forma na comunidade[104].

Com toda a sua estrutura altamente desenvolvida, a atuação do crime organizado representa uma dificuldade acrescida no que diz respeito à produção e recolha de prova, o que determina, em *ultima ratio*, a crescente inadequação dos modos habituais de realização da investigação criminal e, bem assim, de justiça. Atualmente, os meliantes não reconhecem quaisquer fronteiras, atuando a uma escala, volume e envergadura nunca antes vista. Com efeito, como alerta Manuel Augusto Meireis, "*(...) hoje em dia, e pode parecer cruel dizer isto, mas a verdade é que já não é o furto, o rapto isolado, ou mesmo o homicídio que preocupam as mais altas instâncias com competência para definir modelos de prevenção e investigação criminal; (...) o que hoje constitui o principal motivo das suas preocupações, são as novas formas emergentes de criminalidade: os atentados ao ambiente em escala planetária; as grandes redes internacionais de tráfico de droga, de tráfico de armas, de trafico de substâncias radioativas, de tráfico de capitais, de tráfico de obras de arte, de tráfico de órgãos humanos, de tráfico de crianças e de tráfico de embriões. Mas são ainda, e também, os crimes de natureza económica e financeira e, as sempre com eles coligadas, cifras negras; e o incontornável terrorismo*."[105].

Toda a sofisticação inerente aos modos de execução de factos ilícitos por parte da criminalidade organizada determina a clara insuficiência dos meios de investigação criminal atualmente existentes para fazer face a esta delinquência, pelo que se torna necessário recorrer a

[103] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 202;
[104] VALENTE, Manuel Monteiro Guedes, "A Investigação do Crime Organizado – Buscas Domiciliárias Noturnas, O Agente Infiltrado e Intervenção nas Comunicações", In: Centro de Investigação do ISCPSI (Org.), *Criminalidade Organizada e Criminalidade de Massa – Interferências e Ingerências Mútuas*, coordenação de Manuel Monteiro Guedes Valente, Almedina, 2009, pp. 160-161;
[105] MEIREIS, Manuel Augusto Alves, "Homens de Confiança. Será o Caminho?", In: *II Congresso de Processo Penal – Memórias,* coordenação de Manuel Monteiro Guedes Valente, revisão científica de Germano Marques da Silva e Anabela Miranda Rodrigues, Almedina, 2006, p. 83.

novos métodos de investigação que acompanham a evolução gravosa do crime e são, por si só, também eles mais gravosos. O Estado vê-se, assim, obrigado a recorrer a métodos ocultos de investigação para poder prevenir e perseguir esta nova criminalidade, métodos estes que geram grande controvérsia porquanto representam uma elevada restrição de direitos e liberdades fundamentais dos cidadãos.

De acordo com a definição avançada por Manuel da Costa Andrade, os métodos ocultos de investigação criminal traduzem-se no "*(...) conjunto diversificado e heterogéneo de meios de obtenção de conhecimentos, em que os agentes da investigação se intrometem nos processos de comunicação privada das pessoas investigadas, que não têm conhecimento do facto. E, por causa disso, continuam a agir, a interagir e a comunicar de forma espontânea e 'inocente', dizendo e fazendo coisas de conteúdo e sentido direitamente autoincriminatório*."[106]. Para este autor, num grande número de vezes, apenas com o recurso a métodos ocultos de investigação é possível entrar no seio da criminalidade organizada e proceder a uma neutralização dos vínculos de solidariedade que a ligam[107].

Não obstante a eficácia inerente aos meios ocultos de investigação criminal, derivada do facto de os visados acabarem por produzir prova contra si mesmos com total desconhecimento, a verdade é que os meios de obtenção de prova que se inserem nestes métodos, correm à margem dos princípios fundamentais do processo penal de um Estado de Direito, que, pelo contrário, deveria estar preocupado em proteger cada vez mais os direitos e garantias fundamentais dos seus indivíduos[108].

Na senda desta definição, David Silva Ramalho identifica quatro características essenciais dos métodos ocultos de investigação, a saber: o facto de serem totalmente ocultados das pessoas alvos dos mesmos, neutralizando assim alguns dos seus direitos processuais, como o direito à não autoincriminação, derivado do princípio *nemo tenetur se ipsum accusare*; a circunstância de serem bastante abrangentes, por se recolher informações relativas ao presente, passado e futuro e não apenas relativamente a factos compreendidos no período temporal em investigação, envolvendo, de igual modo, terceiros e não apenas o visado; neutralizam o direito de determinadas testemunhas não prestarem o depoimento devido; e, por último, a recolha de informações operada

[106] ANDRADE, Manuel da Costa, "Métodos Ocultos de Investigação (plädoyer para uma teoria geral)", In: *Que futuro para o Direito Processual Penal?, Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (Cordo. Mário Ferreira Monte, Maria Clara Calheiros, Fernando Conde Monteiro, Flávia Noversa Loureiro), Coimbra, Coimbra Editora, 2009, p. 532;
[107] *Idem*, p.. 536;
[108] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, *Bruscamente... A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1ª edição, Rei dos Livros, 2010, p. 37.

não têm em linha de conta a intimidade ou fiabilidade das comunicações observadas ou escutadas[109].

Tratando-se os métodos ocultos de investigação de uma restrição de direitos fundamentais dos cidadãos, torna-se necessário que os mesmos respeitem determinados pressupostos ou requisitos, para que possam ser levados a cabo de uma forma lícita. Como requisitos comuns a todos os métodos ocultos de investigação temos: a reserva de lei; a seleção de um catálogo de infrações criminais; a suspeita fundada; a subsidiariedade; a proporcionalidade; a proibição de aniquilação do âmbito nuclear da intimidade; e a reserva do juiz de instrução.

A reserva de lei impõe que, somente uma lei da Assembleia da República poderá dar concretização legal à adoção de um método oculto de investigação criminal, devendo tal lei identificar concretamente quais os bens jurídicos envolvidos, quais os níveis de sacrifícios que se deverá impor a tais bens jurídicos, quais as técnicas invasivas utilizadas e quais os fundamentos, fins e limites da intromissão na esfera jurídica de cada cidadão. Uma falta de previsão legal implicaria a inexistência de legitimação para utilizar determinado método oculto de investigação, e uma utilização do método oculto sem que para tal esteja legitimado implica uma restrição desproporcionada de direitos fundamentais e, bem assim, uma proibição de prova[110].

A seleção de um catálogo de infrações determina que se adote um catálogo de crimes, suficientemente gravosos, que justifiquem o emprego de um método oculto de investigação e diminuam a danosidade social dos mesmos, devendo igualmente ser adotados critérios de proporcionalidade e restrição dos crimes que legitimam uma medida oculta de obtenção de prova. Caso ocorra a utilização de um método oculto de investigação criminal para a perseguição da prática de um crime não constante do referido catálogo, um crime menos grave, então estaremos perante uma inconstitucionalidade material, por violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa[111].

Por seu turno, a suspeita fundada em factos concretos reporta-se ao facto de não bastar que se esteja perante um crime do catálogo *supra* referido; pelo contrário, torna-se igualmente necessário que exista uma fundada suspeita da prática do crime em apreço e que justifica a utilização de um método oculto de investigação. Esta fundada suspeita deve ter lugar antes do

[109] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 209;
[110] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, Bruscamente... A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 1ª edição, Rei dos Livros, 2010, pp. 53-55;
[111] *Idem*, pp. 55-56.

recurso a uma medida oculta e não deve ser formada num momento posterior, já depois de recolhidos elementos probatórios[112].

O requisito da subsidiariedade dos métodos ocultos de investigação prende-se com a ideia de que deverá ser sempre dada primazia à aplicação de métodos não ocultos de investigação, uma vez que estes últimos são muito menos lesivos dos direitos fundamentais dos indivíduos, assim como representam uma menor devassa da vida privada. Caso seja possível atingir os objetivos da investigação com a utilização de um método não oculto, fica vedada todo e qualquer recurso a métodos ocultos. De igual modo, deverá dar-se prevalência, dentro dos métodos ocultos de investigação, àquele que provocar menos lesões na esfera jurídica do cidadão[113].

No que respeita ao princípio da proporcionalidade, o mesmo impõe que toda a ponderação efetuada em matéria de métodos ocultos de investigação seja norteada pelo mesmo, isto é, quer na seleção dos crimes a integrar no catálogo, quer no grau da suspeita fundada, quer na definição dos níveis de sacrifício a impor aos bens jurídicos deve ter-se em conta a ideia de proporcionalidade em sentido estrito, sendo que a gravidade da intromissão na vida privada dos indivíduos deve ser proporcional às necessidades existentes de investigação criminal e estas devem justificar a utilização de um método oculto de investigação[114].

Já a proibição de aniquilação do âmbito nuclear da intimidade reporta-se ao facto de que, ainda que gravosos, os métodos ocultos não podem nunca interferir os direitos processualmente reconhecidos aos sujeitos processuais. Um qualquer método oculto de investigação que atente contra o núcleo essencial da intimidade ou das garantias processuais penais consagradas deverá ser totalmente omitido e, caso tenha sido iniciado de forma incorreta, deverá ser de imediato interrompido e destruídas todas as provas por meio dele obtidas[115].

Por último, o requisito da reserva do juiz de instrução determina que apenas este poderá dar autorização para o emprego de qualquer método oculto de investigação criminal, entendendo Benjamim Silva Rodrigues que tal competência não pode recair sobre outra entidade, mormente por motivos de urgência, como seja o Ministério Público. Para o autor, o Ministério Público será sempre parte nos autos e terá sempre um interesse na utilização da medida, com o objetivo de atingir uma eficácia investigativa. Cabe ao juiz de instrução assegurar a tutela dos direitos

[112] *Ibidem*;
[113] *Idem*, pp. 57-58;
[114] *Idem*, p. 59;
[115] *Idem*, pp. 60-61;

fundamentais dos cidadãos e, bem assim, evitar o uso de método oculto sempre que entender não se justificar no caso concreto[116].

Como principais métodos ocultos de investigação podemos encontrar atualmente no Código de Processo Penal e em legislação avulsa, a localização e identificação de dados celulares; a localização e identificação a partir de sistemas de GPS; as ações encobertas; as escutas telefónicas; e as informações obtidas através da ingerência corporal.

As ações encobertas, sobre as quais versa o presente estudo e de seguida será dado o devido tratamento, dizem respeito à técnica de, nas palavras de Manuel da Costa Andrade, "*(...) introduzir agentes que, ocultando a sua identidade e os seus propósitos, se intrometem no ambiente das pessoas a investigar e, depois de ganhar a sua confiança ou até a sua amizade, obtêm delas conhecimentos e provas. Podem ser agentes das instâncias formais de controlo, e particularmente da polícia, ou normais terceiros privados.*"[117]. Assumindo um papel crucial para o combate à criminalidade organizada, as ações encobertas permitem um conhecimento aprofundado dos grupos criminosos a partir de dentro, isto é, ao infiltrar-se, o agente acaba por ter uma melhor noção de como opera o grupo, como ocorrem as práticas de factos ilícitos, quais os meios utilizados para tal, sendo benéfico, não só para a recolha de prova com o propósito de prevenir ou iniciar um procedimento criminal contra os autores dos mesmos, mas também para melhor compreender o *modus operandi* deste tipo de organizações e, bem assim, no futuro prevenir a prática de novos crimes por novos grupos.

A elevada importância das ações encobertas resulta patente da consagração das mesmas como técnicas especiais de investigação no n.º 1 do artigo 20.º da Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, igualmente denominada por Convenção de Palermo[118].

2.1. Evolução histórica e legislativa

Nos dias de hoje, assistimos, na doutrina, a uma clara distinção entre os conceitos de agente provocador, agente infiltrado e agente encoberto. Todavia, nem sempre assim foi. Com

---

[116] *Idem*, p. 62;

[117] ANDRADE, Manuel da Costa, "Métodos Ocultos de Investigação (plädoyer para uma teoria geral)", In*: Que futuro para o Direito Processual Penal?, Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (Coord. Mário Ferreira Monte, Maria Clara Calheiros, Fernando Conde Monteiro, Flávia Noversa Loureiro), Coimbra, Coimbra Editora, 2009, p. 534;

[118] Vide n.º 1 do artigo 20.º da Convenção de Palermo, disponível em https://bityli.com/h5Nzi, último acess em 20-07-2021: "*1 - Se os princípios fundamentais do seu ordenamento jurídico o permitirem, cada Estado Parte, tendo em conta as suas possibilidades e em conformidade com as condições previstas no seu direito interno, deverá adotar as medidas necessárias para permitir o recurso apropriado a entregas controladas e, quando o considere adequado, o recurso a outras técnicas especiais de investigação, como a vigilância eletrónica ou outras formas de vigilância e as ações encobertas, por parte das autoridades competentes no seu território, a fim de combater eficazmente a criminalidade organizada.*".

efeito, aquando do aparecimento da figura do agente provocador, a ele eram chamadas todas as diferentes formas de intervenção do mesmo, tratando-se, assim, de um conceito extremamente amplo e abrangente.

Este conceito amplo de *agent provocateur*, surgiu em França, no seio do Antigo Regime, o *Ancién Regime*, onde a onda de criminalidade existente era cada vez maior e se tornava, a cada dia que passava, mais difícil de combater e controlar. Nesta senda, foram criados, em 1708, os denominados inspetores de polícia que, dado o enorme fluxo de trabalho, viam-se obrigados a recorrer a terceiros, trabalhando alguns destes clandestinamente para os referidos inspetores, e outros eram efetivamente contratados e encarregados de executar determinadas tarefas. Tal fez deles os primeiros agentes provocadores que a Europa viu nascer. Aos que trabalhavam encobertos, de forma clandestina, era lhes atribuída a denominação de *observateurs*, e aos que eram, de forma pública, contratados, a designação de *mouches*, sendo que estes últimos eram, frequentemente, reclusos que, através da sua infiltração em lugares e ambientes perigosos, negociavam com os inspetores da polícia a sua liberdade. Não obstante o recurso a estes agentes ocorresse em quase todos os setores da criminalidade, mais tarde, com a Revolução Francesa, em 1789, o governo passou igualmente a ter interesse na sua utilização, com o intuito de se poder livrar de certas pessoas que incomodavam e não podiam ser condenadas pela prática de crimes, dada a insuficiência de prova[119].

Deste conceito histórico de *agent provocateur* é possível identificar diferentes formas de atuação, como as apontadas por Isabel Oneto: "*(...) o agente podia ser contratado para se infiltrar (agente infiltrado) ou ser pago para seguir, escutar e informar, como para provocar a comissão do crime (agente provocador), além daquele que negociava a sua liberdade a troco de cooperação (informador)*."[120], sendo patente a estreita relação de proximidade que era mantida entre os diferentes agentes e os órgãos de polícia criminal, na medida em que uns necessitavam de outros – os agentes para conseguirem a tão esperada liberdade e os órgãos de polícia para conseguirem travar a crescente criminalidade e, bem assim, condenar os meliantes pela prática de factos ilícitos.

Apesar de, historicamente, a figura do *agent provocateur* ter aparecido em França, a delimitação conceptual e jurídica do mesmo apenas ocorreu mais tarde, na Alemanha, por intermédio de Julius Glaser que, em 1858, fez uma abordagem abstrata a esta figura e rompe

[119] MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas Pelo Agente Provocador em Processo Penal*, Coimbra, Almedina, 1999, pp. 19-21;
[120] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, p. 22.

definitivamente com a referência maioritária da utilização do agente provocador em demandas políticas[121]. De acordo com a teoria apresentada por Glaser, não só tanto um particular como um agente pertencente às instâncias formais da polícia podem atuar como um agente provocador, como, nas palavras de Luiz Ruiz Anton "*El agente provocador criminal, mediante la incitación de acciones delictivas, no persigue ni para sí ni para otro la obtención del resultado gratificador que se supone comporta al delincuente la realización del delito, sino por el contrario lo único que pretende, de modo inmediato, es la denuncia y el castigo de la persona provocada*."[122].

No entendimento de Manuel Augusto Meireis, a tese de Glaser constituiu o mote para o desenvolvimento da noção de agente provocador, que ocorreu ao longo de duas fases distintas, uma fase dogmática ou monista e uma fase pluralista ou criminológica. A fase dogmática ou monista decorreu desde as origens oitocentistas até meados dos anos 70, no âmbito da qual existia uma noção unitária de agente provocador, tanto para a doutrina como para a jurisprudência. Apesar de não legalmente prevista, a figura do agente provocador era considerada uma problemática e originando da expressão francesa *agent provocateur*, surge a expressão alemã *Lockspitzel*, tendo Glaser definido este como "*(...) aquele instigador que determina outrem à perpetração de um crime apenas porque quer que este seja acusado e punido*.". Posteriormente, com a fase pluralista ou criminológica, começam a surgir novas figuras da prática criminal e da jurisprudência dos tribunais superiores, que começam, por sua vez, a ser tipificadas pelo legislador, sendo, a partir deste momento, que surge a expressão *Vertrauens-Männer*, os denominados homens de confiança[123].

Para Manuel da Costa Andrade, neste conceito inserem-se "*(...) todas as testemunhas, que colaboram com as instâncias formais de perseguição penal, tendo como contrapartida a promessa de confidencialidade da sua identidade e atividade. Cabem aqui tanto os particulares (pertencentes ou não ao submundo da criminalidade) como os agente das instâncias formais, nomeadamente da polícia, que disfarçadamente se introduzem naquele submundo ou com ele entram em contacto; e quer se limitem à recolha de informações, quer vão ao ponto de provocar eles próprios a prática do crime*."[124].

Por seu turno, no Reino Unido, o recurso ao agente provocador sempre foi uma prática recorrente, em que, para encorajar a retirada de criminosos da sociedade, eram entregues

[121] ANTON, Luis Felipe Ruiz, *El Agente Provocador en el Derecho Penal*, Madrid, Editoriales de Derecho Reunidas, 1982, p. 24;
[122] *Ibidem*;
[123] MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas Pelo Agente Provocador em Processo Penal*, Coimbra, Almedina, 1999, pp. 24-26.
[124] ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, 1992, p. 220;

recompensas e imunidades àqueles que os fizessem chegar à justiça. O pagamento destes prémios era entendido como um incentivo e uma forma de levar o povo a participar no combate ao crime, o que acabaria por diminuir, de forma drástica, a taxa de criminalidade. Este sistema de recompensas atribuídas pelo parlamento britânico acabou por ser abolido pelo *Bennet's Act*, em 1816, que transferiu para o poder judiciário esta faculdade de atribuir prémios. Não obstante este constante recurso à figura do agente provocador, a verdade é que a expressão *agent provocateur* apenas foi oficialmente reconhecida em 1928, "*(...) quando a Royal Commission on Police Powers o definiu como aquele que 'incita outrem a cometer uma determinada transgressão da lei que de outra maneira não teria cometido e depois testemunha contra ela no âmbito dessa infração'.*"[125].

Em Portugal, a primeira abordagem ao agente infiltrado surgiu com o Decreto-Lei n.º 430/83 de 13 de Dezembro, também denominado por Lei da Droga, onde no n.º 1 do seu artigo 52.º, sob a epígrafe *Conduta não punível*, se podia ler que: "*Não é punível a conduta do funcionário de investigação criminal que, para fins de inquérito preliminar, e sem revelação da sua qualidade e identidade, aceitar diretamente ou por intermédio de um terceiro a entrega de estupefacientes ou substâncias psicotrópicas.*"[126]. Posteriormente, o Decreto-Lei n.º 15/93, de 22 de Janeiro, introduziu várias alterações à Lei da Droga, entre as quais consagrou o regime das entregas controladas, no artigo 61.º, de acordo com o qual era concedida aos órgãos de polícia criminal a prorrogativa de não atuar sobre indivíduos portadores de estupefacientes ou substâncias psicotrópicas, com o intuito de, mais tarde, poder identificar um número maior de participantes, mormente, relacionados com grandes redes de tráfico[127]. De igual modo, equiparou, nos termos do disposto no n.º 1 do artigo 51.º, o tráfico de droga, para efeitos de perseguição penal, a casos de terrorismo, criminalidade violenta ou altamente organizada.

De seguida, a Lei n.º 36/94, de 29 de Setembro, relativa às Medidas de Combate à Corrupção e Criminalidade Económica e Financeira, veio, de acordo com o artigo 6.º, legitimar o recurso a agentes infiltrados no âmbito da investigação criminal realizada à prática dos crimes previstos no n.º 1 do artigo 1.º do referido diploma legal[128]. Mais tarde, com a entrada em vigor da Lei n.º 45/96, de 03 de Setembro, assistimos a um alargamento do âmbito de atuação dos

---

[125] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, pp. 24-25;

[126] Disponível em https://bityli.com/9hU66, último acesso em 23-07-2021;

[127] Disponível em https://bityli.com/iM645, último acesso em 23-07-2021. Vide artigo 61.º n.º 1: "*Pode ser autorizada, caso a caso, pelo Ministério Público, a não atuação da Polícia Judiciária sobre os portadores de substâncias estupefacientes ou psicotrópicas em trânsito por Portugal, com a finalidade de proporcionar, em colaboração com o país ou países destinatários e outros eventuais países de trânsito, a identificação e arguição do maior número de participantes nas diversas operações de tráfico e distribuição, mas sem prejuízo do exercício da ação penal pelos factos aos quais a lei portuguesa é aplicável.*".

[128] Disponível em https://bityli.com/PQnd4, último acesso em 23-07-2021;

agentes infiltrados na prevenção e repressão de determinados crimes relacionados com o tráfico de estupefacientes e substâncias psicotrópicas, tendo o artigo 59.º-A sido a primeira referência expressa, num diploma legal, à figura do agente infiltrado e à intervenção de terceiros como agentes infiltrados[129].

No entendimento de Rui Pereira, foram cinco as principais alterações introduzidas pelo diploma legal vindo de referir, a saber: a admissão de o agente infiltrado poder agora aceitar, deter, guardar, transportar e entregar droga, ao passo que, na vigência da lei anterior, apenas podia aceitar; a exigência de autorização prévia por parte da autoridade judiciária competente para a infiltração, sendo, contudo, esta dispensada em caso de urgência, desde que validada no primeiro dia útil posterior; o alargamento do prazo de que dispunha a Polícia Judiciária para apresentar o relato da intervenção, de 24 horas para 48 horas; a restrição de junção ao processo do referido relato aos casos em que tal fosse considerado indispensável, em termos probatórios; e, por último, a exclusão de publicidade da audiência de discussão e julgamento sempre que nela fosse comparecer e participar o agente infiltrado[130]. De acordo com o autor, "*(...) foi a Lei n.º 45/96 que introduziu em Portugal um regime minimamente elaborado sobre o 'agente encoberto'*."[131].

Atualmente, a Lei n.º 101/2001, de 25 de Agosto, estabelece o Regime Jurídico das Ações Encobertas para Fins de Prevenção e Repressão Criminal, tendo revogado expressamente os artigos 59.º e 59.º-A da Lei n.º 15/93 e o artigo 6.º da Lei n.º 36/94.

2.2. Delimitação dos conceitos de agente provocador, infiltrado e encoberto

No contexto das ações encobertas, é frequente assistir-se ao emprego de várias expressões para denominar a pessoa que desempenha o papel de sujeito ativo no âmbito das mesmas, sejam elas *agente provocador*, *agente infiltrado* ou *agente encoberto*, sendo particularmente importante compreender, no presente estudo, se tais expressões podem ser usadas de forma indistinta ou se, pelo contrário, designam diferentes realidades.

---

[129] Disponível em https://bityli.com/O4huX, último acesso em 23-07-2021. Vide artigo 59.º-A:
"*1 - A autoridade judiciária só ordenará a junção ao processo do relato a que se refere o n.º 4 do artigo anterior se a reputar absolutamente indispensável em termos probatórios.*
2 - A apreciação da indispensabilidade pode ser remetida para o termo do inquérito ou da instrução, ficando entretanto o expediente, mediante prévio registo, na posse da Polícia Judiciária.
3 - No caso de o juiz determinar, por indispensabilidade da prova, a comparência em audiência de julgamento do funcionário ou do terceiro infiltrados, observará sempre o disposto na segunda parte do n.º 1 do artigo 87.º do Código de Processo Penal.";

[130] PEREIRA, Rui, "O 'Agente Encoberto' na Ordem Jurídica Portuguesa", In: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, p. 23;

[131] *Idem*, p. 24.

Relativamente à figura do agente provocador, António Henriques Gaspar define-a como "*(...) 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 desejo de obter provas da prática desse crime ou de submeter o autor do facto a um processo penal e à condenação.*"[132]. O papel do agente provocador não é, assim, o de um mero observador ou acompanhante das decisões prévia e autonomamente tomadas pelo meliante, mas sim, desempenha um verdadeiro papel decisivo na formação da vontade do criminoso em proceder à prática de um facto ilícito. Para o autor, ao suscitar a infração, o agente provocador torna-se num autor imediato do crime, fazendo nascer ou reforçando a resolução criminosa[133].

Por seu turno, Manuel Augusto Meireis entende que o agente provocador é "*(...) aquele que, sendo um cidadão particular ou entidade policial, convence outrem à prática de um crime não querendo o crime a se, e, sim, pretendendo submeter esse outrem a um processo penal e, em último caso, a uma pena.*"[134]. De acordo com a tese defendida pelo autor, a qualidade do agente, isto é, se se trata de um agente de autoridade ou de um terceiro particular, é irrelevante para a definição do conceito de agente provocador. A pedra de toque nesta delimitação concetual reside em saber se o agente tinha a intenção de, através das suas ações, levar outrem à prática de um crime e se, mesmo tendo-o provocado, não queria que o crime tivesse tido lugar. Deverá existir um dolo quanto à determinação de outrem à prática de um facto ilícito, mas não poderá existir dolo quanto ao crime propriamente dito. No que respeita à atuação do agente provocador, qualquer ação deste que seja adequada a impulsionar outrem à prática de um crime torna-se relevante para a sua classificação como agente provocador, sendo que a atuação deste terá uma finalidade primária, direta ou imediata quando o agente pretender a condenação do indivíduo provocado só mesmo pela condenação; ou uma finalidade secundária, indireta e mediata quando o agente provocador encarar a condenação como um meio para atingir um fim[135].

No que respeita à jurisprudência dos tribunais superiores, o Supremo Tribunal de Justiça definiu, em 1999, o agente provocador como "*(...) um membro da autoridade policial, ou um civil comandado pela polícia, induz outrem a delinquir por forma a facilitar a recolha de provas da ocorrência do ato criminoso.*"[136]. Já mais recentemente, em 2010, o Tribunal da Relação de Évora pronunciou-se acerca deste conceito, entendendo que "*O agente provocador é assim, em qualquer*

---

[132] GASPAR, António Henriques, "As Ações Encobertas e o Processo Penal", In: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, p. 46;
[133] *Idem*, p. 47;
[134] MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas Pelo Agente Provocador em Processo Penal*, Coimbra, Almedina, 1999, p. 155.
[135] *Idem*, pp. 155-156;
[136] Vide acórdão datado de 13-01-1999, relativo ao processo n.º 98P999, disponível em https://bityli.com/FHKjC, último acesso em 26-07-2021;

circunstância, aquele que determina outrem à prática do crime, toma, por qualquer meio, a iniciativa e provoca uma atividade criminosa que, sem ela não teria lugar. O agente provocador induz à prática de atos ilícitos, criando ele próprio as condições para a verificação de uma nova infração, pela qual o provocado será incriminado. O agente provocador, atuando sobre uma falsa identidade e sem revelar a sua verdadeira qualidade, fazendo-se passar por quem não é, convence outrem à prática do crime."[137].

Não obstante as pequenas variações nas definições avançadas pelos diversos autores e pela jurisprudência dos tribunais superiores, como denominador comum temos sempre a necessidade de existência de um nexo de causalidade. Isto é, só estaremos perante uma situação de provocação se existir um nexo de causalidade entre o agente provocador e a conduta levada a cabo pelo indivíduo provocado, na medida em que, se não ocorresse determinada ação por parte do agente provocador, não teria sido cometido um crime.

O emprego da provocação para, posteriormente, proceder à recolha de prova com o intuito de fundamentar uma condenação do sujeito provocado e consequente aplicação de pena, suscita muitas preocupações no seio da doutrina e da jurisprudência, que o tem vindo a rejeitar veemente, por atentar contra os princípios mais básicos do processo penal característico de um Estado de Direito, como sejam o princípio democrático e o princípio da lealdade.

De acordo com o princípio democrático, todos os órgãos de polícia criminal deverão atuar no respeito pela dignidade da pessoa humana, na igualdade de todos os cidadãos perante a lei, devendo todos ser encarados como seres humanos e não como potenciais criminosos, logo à partida. Nesta senda, Germano Marques da Silva defende que, apenas numa *conceção aristocrática* de sociedade, se poderia considerar o recurso à provocação como um método legítimo de combate à criminalidade organizada, caso em que se aceitaria a existência de pessoas predispostas, por natureza, para a prática de crimes, o que não se pode conceder. Deverá excluir-se a provocação como método de investigação criminal e meio de obtenção de prova, por esta não ser informativa, mas sim totalmente formativa, criando o crime e o criminoso, e não apenas revelando-os, como finalidade da própria investigação criminal. Para o autor, "*Há que ponderar que a ordem pública é mais perturbada pela violação de regras fundamentais da dignidade e da retidão da atuação judiciária, pilares fundamentais da sociedade democrática, do que pela não repressão de alguns crimes, por mais graves que sejam, pois são sempre muitos, porventura a*

[137] Vide acórdão datado de 04-02-2010, relativo ao processo n.º 196/08.3JAFAR.E1, disponível em https://bityli.com/VPeoU, último acesso em 27-07-2021.

maioria, os que não são punidos, por não descobertos, sejam quais forem os métodos de investigação utilizados."[138].

Já o princípio da lealdade determina um total respeito pelos princípios gerais adstritos à própria ideia de dignidade da pessoa humana e de ética, devendo ser dada aos cidadãos a possibilidade de se submeterem a um processo justo. De igual modo defensores da inadmissibilidade legal da utilização do agente provocador, Fernando Gonçalves, Manuel João Alves e Manuel Guedes Valente entendem não se alcançar o devido respeito pelos valores próprios da pessoa humana quando os órgãos de polícia criminal se socorrem de meios de obtenção de prova que violam um dos pilares mais fundamentais do processo penal – o respeito pela dignidade da pessoa humana –, como é o caso da provocação. Entendem os autores que "*O procedimento leal por parte dos operadores judiciários proíbe que estes façam uso de métodos proibidos, como a provocação na recolha de provas, porque o suspeito (arguido) nunca poderá ser tratado como um objeto, melhor, como um meio de prova utilizado contra si mesmo (...)*"[139].

No mesmo sentido, seguem Susana Aires de Sousa e Manuel Augusto Meireis, entendendo estes que a utilização da provocação como método de investigação criminal não se coaduna com a ideia de *due process* e com o princípio *nemo tenetur se ipsum accusare*, não se podendo tolerar a atuação de um Estado que, nas suas vestes de polícia, fomenta a prática do crime para, posteriormente, já nas suas vestes de tribunal, proceder ao respetivo julgamento e condenação[140].

Entre nós, entendemos não se poder perfilhar de outra opinião que não das *supra* expostas, na medida em que o combate à criminalidade organizada não pode fazer-se de modo desregrado e num total desrespeito pelos princípios fundamentais do Estado de Direito democrático e de um processo penal de estrutura acusatória mitigada pelo princípio da investigação material. Apesar de uma das finalidades do processo penal ser a de atingir a verdade material, a busca por esta não pode ocorrer com recurso a um meio de obtenção de prova que provoca, ele próprio, a prática do crime, que até poderia não ter lugar caso não existisse uma atuação por parte do agente provocador. A utilização de um tal método de investigação criminal

[138] SILVA, Germano Marques da, "Bufos, Infiltrados, Provocadores e Arrependidos – Os Princípios Democráticos e da Lealdade em Processo Penal", In: BELEZA, Teresa Pizarro (Org.), *Apontamentos de Direito Processual Penal*, III Vol., Lisboa, Associação Académica da Faculdade de Direito de Lisboa, 1995, p. 64;

[139] GONÇALVES, Fernando, ALVES, Manuel João, e VALENTE, Manuel Monteiro Guedes, *O Novo Regime Jurídico do Agente Infiltrado, Comentado e Anotado – Legislação Complementar*, Almedina, 2001, pp. 32-34;

[140] Vide SOUSA, Susana Aires de, "Agent Provocateur e Meios Enganosos de Prova. Algumas Reflexões", In: ANDRADE, Manuel da Costa, COSTA, José de Faria, RODRIGUES, Anabela Miranda, e ANTUNES, Maria João (Org.), *Liber Discipulorum para Jorge de Figueiredo Dias*, Coimbra Editora, 2003, p. 1234; e MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas Pelo Agente Provocador em Processo Penal*, Coimbra, Almedina, 1999, p. 249.

redundaria numa situação insustentável – aquela em que o Estado promove a prática de crimes para posteriormente poder punir os seus agentes.

Tendo em conta as referidas opiniões acerca da (in)admissibilidade da utilização da provocação como método de investigação criminal e como meio de obtenção de prova, a doutrina têm sido unânime ao entender que as provas obtidas pelo agente provocador devem ser consideradas provas proibidas, por inadmissíveis relativamente ao artigo 125.º do Código de Processo Penal, sendo, de igual modo, reconduzíveis aos métodos proibidos de prova, nos termos da alínea a) do n.º 2 do artigo 126.º do aludido diploma legal, pelo que são nulas e não podem ser utilizadas[141]. Neste sentido segue também a jurisprudência dos tribunais superiores, tendo o Tribunal Constitucional entendido, já em 1998, 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.*"[142].

No que se refere à figura do agente provocador, cumpre, por último, fazer referência ao célebre acórdão do Tribunal Europeu dos Direitos do Homem, relativo ao caso *Teixeira de Castro vs. Portugal*, no âmbito do qual foi proferida a 1ª decisão condenatória de Portugal em matéria da atuação de agente provocador. Com efeito, Portugal foi condenado por violação do artigo 6.º da Convenção Europeia dos Direitos do Homem, em virtude de o tribunal ter considerado que a recolha de prova que levou à condenação do arguido Francisco Teixeira de Castro pela prática do crime de tráfico de estupefacientes, à data punível pelos artigos 23º e 27º, alíneas h) e c) do Decreto-Lei nº 430/83, resultou da atuação de dois agentes da Polícia de Segurança Pública, que atuaram como agentes provocadores, não tendo o arguido tido direito a um processo equitativo[143].

Distinta do agente provocador é a figura do agente infiltrado que, de acordo com a definição avançada por Manuel Augusto Meireis se traduz no "*(...) agente da autoridade ou cidadão particular (mas que atue de forma concertada com a polícia) que, sem revelar a sua identidade ou*

---

[141] GONÇALVES, Fernando, ALVES, Manuel João, e VALENTE, Manuel Monteiro Guedes, *Lei e Crime: O Agente Infiltrado Versus o Agente Provocador – Os Princípios do Processo Penal*, Almedina, 2001, p. 261;

[142] Vide acórdão n.º 578/98, relativo ao processo n.º 835/98, de 14 de Outubro, disponível em https://bityli.com/nXZaI, último acesso em 27-07-2021;

[143] Vide LOUREIRO, Joaquim, *Agente Infiltrado? Agente Provocador! – Reflexões sobre o 1.º Acórdão do T.E.D. Homem – 9.Junho.1998. Condenação do Estado Português*, Almedina, 2007, p. 168-173. Consta da fundamentação do acórdão que: "*33. The Commission considered that the offence had been committed and the applicant sentenced to what was a fairly heavy penalty essentially, if not exclusively, as a result of the police officers' actions. The officers had thus incited criminal adtivity which might not otherwise have taken place. That situation had irremediably affected the fairness of the proceedings. (...) 39. In the light of all these considerations, the Court concludes that the two police officers' actions went beyond those of undercover agentes 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.*";

qualidade e com o fim de obter provas para a incriminação do(s) suspeito(s), ou então simplesmente, para a obtenção da notitia criminis, ganha a sua confiança pessoal, mantendo-se a par dos acontecimentos, acompanhando a execução dos factos, praticando atos de execução se necessário for, por forma a conseguir a informação necessária ao fim que se propõe.". Para o autor, o essencial para a caracterização da figura do agente infiltrado é a obtenção da confiança do criminoso ou de uma rede criminosa, tornando-se assim o infiltrado, de modo aparente, apenas mais uma pessoa a ela pertencente, tudo com o objetivo de ter acesso direto a informações privilegiadas que, em *ultima ratio*, se vão consubstanciar em provas para sustentar uma condenação penal[144].

A circunstância de o agente infiltrado se tornar, no seio da sua operação, um mero *peer* dos criminosos, poderá resultar no facto de o mesmo ter que praticar atos de execução tendentes à prática de crimes. Nesta senda, defende o referido autor e, de igual modo, a grande maioria da doutrina, que a atuação do agente infiltrado poderá revestir uma forma de autoria e uma forma de participação: a coautoria e a cumplicidade, respetivamente. Nunca caberá ao agente infiltrado instigar ou determinar outra pessoa à prática de um facto ilícito, sendo-lhe apenas permitido prestar o necessário auxílio moral e material, nos termos do disposto no n.º 1 do artigo 26.º do Código Penal[145].

Já para Isabel Oneto, o agente infiltrado não é só um simples observador, mas sim um verdadeiro participante ativo da atividade criminosa. Inserindo-se no seio da criminalidade, convivendo com os meliantes e ganhando a sua confiança, o agente infiltrado é, para a autora, "*(...) o agente policial, ou terceiro sob a orientação daquele, que, no âmbito da prevenção ou repressão criminal, e com o fim de obter provas incriminatórias sobre determinadas atividades criminosas, oculta a sua identidade e qualidade, podendo praticar factos típicos sem, contudo, os poder determinar*."[146].

Das definições apresentadas é possível verificar que a figura do agente infiltrado se distingue claramente do conceito de agente provocador, *supra* analisado, distinção esta que terá, necessariamente, que assentar em critérios relativos ao grau de intervenção da atuação do agente no desenrolar dos factos dolosos e qual o contributo do mesmo para a formação da vontade do criminoso em proceder à prática de tais factos[147]. Com efeito, ao passo que o agente infiltrado se

---

[144] MEIREIS, Manuel Augusto Alves, *O Regime das Provas Obtidas Pelo Agente Provocador em Processo Penal*, Coimbra, Almedina, 1999, pp. 163-164;
[145] *Ibidem*.
[146] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, p. 150;
[147] PEREIRA, Sandra, "A Recolha de Prova por Agente Infiltrado", In: *Prova Criminal e Direito de Defesa – Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal*, coordenação de Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, 2010, p. 143;

limita a acompanhar a execução dos crimes e, no limite, pratica atos de execução dos mesmos, o agente provocador intervém diretamente no processo de formação da vontade do criminoso, isto é, o agente provocador faz com que nasça ou se desenvolva ativamente no criminoso a vontade de cometer um crime, crime este que, sem a atuação do provocador, provavelmente não teria ocorrido. Concordamos, assim, com Manuel Augusto Meireis, no entendimento fundamental do conceito de agente infiltrado reside a característica da obtenção da confiança do criminoso, porque, na verdade, é isto que o agente infiltrado se limita a fazer, ganha a confiança do criminoso para depois poder obter provas da prática do crime; prática contrária à do agente provocador que incentiva e impulsiona a prática do crime pelo provocado.

No que concerne à admissibilidade da figura do agente infiltrado, a doutrina e a jurisprudência dos tribunais superiores tem vindo a entender que a mesma deve ser admitida, desde que respeite alguns requisitos, mormente os já *supra* evidenciados quanto à aplicação de métodos ocultos de investigação, como sejam a previsão legal, com o intuito de garantir a tutela efetiva dos direitos fundamentais dos cidadãos; a adequação e proporcionalidade da utilização do agente infiltrado face às necessidades de prevenção e repressão criminal; e a subsidiariedade do recurso ao mesmo, na medida em que apenas deve ocorrer quando outros, menos onerosos, não produzam os efeitos desejados[148]. Defende Manuel Augusto Meireis que o emprego do agente infiltrado deve integrar o catálogo de métodos de prova relativamente proibidos, nos termos do disposto nos artigos 32.º n.º 8 da Constituição da República Portuguesa e 126.º n.º 3 do Código de Processo Penal, sendo que, em caso de desrespeito pelo conteúdo do artigo 18.º da Constituição da República Portuguesa, estaremos perante uma intromissão abusiva na vida privada dos cidadãos, o que consubstancia uma conduta ilícita, um método proibido de prova e a obtenção de provas nulas[149].

Novamente em total acordo com o autor, entendemos que o recurso a agentes infiltrados se torna, na sociedade atual, em que a criminalidade organizada tem vindo a crescer exponencialmente, um elemento essencial para prevenir e reprimir a mesma, não se podendo, contudo, olvidar que há preceitos normativos que têm, imperativamente, que ser observados, sob pena de nos encontrarmos num plano em que a busca pela verdade material tem primazia sobe o respeito pelos direitos, liberdades e garantias de que dispõem os cidadãos.

---

[148] VALENTE, Manuel Monteiro Guedes, "A Investigação do Crime Organizado – Buscas Domiciliárias Noturnas, O Agente Infiltrado e Intervenção nas Comunicações", In: Centro de Investigação do ISCPSI (Org.), *Criminalidade Organizada e Criminalidade de Massa – Interferências e Ingerências Mútuas*, coordenação de Manuel Monteiro Guedes Valente, Almedina, 2009, pp. 173-174.

[149] MEIREIS, Manuel Augusto Alves, "Homens de Confiança. Será o Caminho?", In: II *Congresso de Processo Penal – Memórias*, coordenação de Manuel Monteiro Guedes Valente, revisão científica de Germano Marques da Silva e Anabela Miranda Rodrigues, Almedina, 2006, pp. 95-96;

Por último, no que diz respeito ao agente encoberto, Fernando Gonçalves, Manuel João Alves e Manuel Guedes Valente defendem que, numa aceção totalmente distinta do agente provocador e do agente infiltrado, o mesmo é "*(...) um órgão de polícia criminal (da Polícia Judiciária, da Polícia de Segurança Pública ou da Guarda Nacional Republicana) ou o particular que, de forma concertada com ele atua, que, sem revelar a sua qualidade ou identidade, frequenta os lugares conotados com o crime, (..), com a finalidade de identificar, e eventualmente deter, possíveis suspeitos da prática de crimes, mais ou menos graves, de natureza pública ou semipública, sem contudo, determinar a prática de qualquer crime ou conquistar a confiança de alguém.*"[150]. Seguindo a mesma linha de pensamento que Manuel Augusto Meireis, os autores defendem que a principal característica do agente encoberto é a absoluta passividade com que atua relativamente à decisão criminosa, sendo a sua presença no meio do crime indiferente para a determinação do rumo dos acontecimentos. Encontrando-se a decisão criminosa e a prática dos factos de execução do crime à mercê da iniciativa do delinquente, o risco corre totalmente por conta deste último, que é meramente observado pelo agente encoberto[151].

Numa perspetiva oposta, Isabel Oneto entende que o agente encoberto "*(...) é aquele que pode ocultar a sua qualidade ou identidade no seu relacionamento com terceiros, mantendo-os na ignorância para ganhar a sua confiança.*", desempenhando, nesta medida, o mesmo papel que o agente infiltrado, daí que, para a autora, não haja uma verdadeira distinção entre os dois conceitos; e, a existir, seria sempre na ótica de que o agente encoberto é uma subespécie de agente infiltrado. Apesar de o legislador ter optado pela consagração, na Lei n.º 101/2001, que estabelece o Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal, da expressão *agente encoberto*, em detrimento da expressão *agente infiltrado*, inclui-se na primeira uma realidade que abrange as suas figuras[152].

Entre nós, aderimos à tese defendida por Isabel Oneto, porquanto da atenta análise da referida Lei n.º 101/2001, que *infra* se passará a expor, não nos parece que o legislador tenha tido a intenção de proceder a tal distinção; pelo contrário, entendemos que se encontram previstas tanto situações em que o agente tem um papel mais interventivo, como aquelas em que este apenas observa a prática de crimes. Outro entendimento não nos parece possível, até porque, caso se entendesse que o agente encoberto apenas observa a prática de factos ilícitos para,

[150] GONÇALVES, Fernando, ALVES, Manuel João, e VALENTE, Manuel Monteiro Guedes, *O Novo Regime Jurídico do Agente Infiltrado, Comentado e Anotado – Legislação Complementar*, Almedina, 2001, pp. 40-41;
[151] MEIREIS, Manuel Augusto Alves, O Regime das Provas Obtidas Pelo Agente Provocador em Processo Penal, Coimbra, Almedina, 1999, pp. 192-193.
[152] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, pp. 139-141;

posteriormente, atuar, não se compreende a previsão, no n.º 1 do artigo 6.º da Lei n.º 101/2001, da isenção de responsabilidade do mesmo quando pratique atos preparatórios ou de execução de uma infração[153].

2.3. Regime jurídico das ações encobertas

Conforme já *supra* exposto, o Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal, doravante designado por Regime Jurídico das Ações Encobertas, foi introduzido no ordenamento jurídico português com a Lei n.º 101/2001, de 25 de Agosto[154].

No seu n.º 1 do artigo 1.º, refere-se, conforme advém do título da mesma, que o Regime Jurídico das Ações Encobertas consagrado abrange as finalidades de prevenção e investigação criminal. Tal significa que o legislador limitou, deliberadamente, o recurso ao agente encoberto às aludidas finalidades. Apesar de a finalidade de investigação criminal não suscitar problemas de maior, o mesmo não se poderá dizer em relação à finalidade de prevenção.

Nesta senda, Fernando Gonçalves, Manuel João Alves e Manuel Guedes Valente alertam para o facto de ter ficado por clarificar se as finalidades de prevenção previstas se reportam a uma prevenção criminal *lato sensu*, em que se insere a atividade de vigilância e de prevenção criminal *stricto sensu*; ou, então, se apenas se reporta a uma prevenção *stricto sensu*. Para os autores, os princípios da subsidiariedade, exceção e proporcionalidade impõem que o recurso ao agente encoberto apenas possa ter lugar quando à prevenção criminal *stricto sensu*, traduzindo-se esta na adoção de medidas adequadas para combater determinadas infrações de natureza criminal, sem que, contudo, ocorra uma limitação do exercício de direitos, liberdades e garantias dos cidadãos[155]. Por seu turno, Benjamim Silva Rodrigues, demonstrando o seu claro desagrado com o instituto jurídico em apreço, aponta para a conclusão que retira da perseguição de finalidades de prevenção com o recurso ao agente encoberto – a de ser possível que as ações encobertas ocorram à margem de um qualquer procedimento criminal 'em curso'[156].

---

[153] Vide artigo 6.º n.º 1 da Lei n.º 101/2001: "*1 - 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.*";

[154] Disponível em https://bityli.com/OPrL0, último acesso em 28-08-2021.

[155] GONÇALVES, Fernando, ALVES, Manuel João, e VALENTE, Manuel Monteiro Guedes, *O Novo Regime Jurídico do Agente Infiltrado, Comentado e Anotado – Legislação Complementar*, Almedina, 2001, pp. 28-29;

[156] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, *Bruscamente... A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1ª edição, Rei dos Livros, 2010, p. 124;

Quanto a nós, partilhamos do entendimento perfilhado por Sandra Pereira, de acordo com o qual, mais do que saber quais os tipos de atividade em causa, se repressiva, se preventiva, é necessário ter em conta o grau de lesão que o recurso a um tal meio excecional de obtenção de prova provoca nos princípios constitucionais de garantia no processo penal[157]. Com efeito, apesar de entendermos que as ações encobertas podem ser realizadas com uma finalidade preventiva, cremos que o respeito pelos direitos fundamentais dos cidadãos deve sempre nortear todo a operação, só se podendo recorrer à mesma quando inexistir um outro meio de obtenção de prova menos gravoso e menos lesivo.

O n.º 2 do artigo 1.º do Regime Jurídico das Ações Encobertas delimita o âmbito subjetivo das ação encobertas, ao determinar que estas são "*(...) aquelas que sejam 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.*". No que se refere à possibilidade de o agente encoberto ser um funcionário de investigação criminal, cumpre esclarecer que apenas poderão atuar como agentes encobertos os funcionários de investigação criminal da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras e não os pertencentes à Polícia de Segurança Pública ou Guarda Nacional Republicana. Isto porque a competência para investigar os crimes previstos no artigo 2.º do Regime Jurídico das Ações Encobertas pertence, exclusivamente à Polícia Judiciária, nos termos do disposto no artigo 7.º da Lei n.º 49/2008, de 27 de Agosto, também designada por Lei da Organização da Investigação Criminal. Mais recentemente, com a entrada em vigor da Lei n.º 23/2007, de 04 de Julho, também o Serviço de Estrangeiros e Fronteiras têm competência para investigar os referidos crimes, de acordo com o artigo 188.º do referido diploma legal[158]. Não obstante o artigo 8.º da Lei da Organização da Investigação Criminal preveja a possibilidade de o Procurador-Geral da República deferir a investigação de determinado crime, que se encontrava adstrita à Polícia Judiciária, a outro órgão de polícia criminal, parece-nos que, no que respeita às ações encobertas, apenas poderá ser agente encoberto um funcionário de investigação criminal da Polícia Judiciária. Outro entendimento não se nos afigura possível porquanto, se assim não fosse, não existiriam

[157] PEREIRA, Sandra, "A Recolha de Prova por Agente Infiltrado", In: *Prova Criminal e Direito de Defesa – Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal*, coordenação de Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, 2010, p. 147.

[158] Vide artigo 188.º da Lei n.º 23/2007:

"*1 - Além das entidades competentes, cabe ao SEF investigar os crimes previstos no presente capítulo e outros que com ele estejam conexos, nomeadamente o tráfico de pessoas.*

2 - As ações encobertas desenvolvidas pelo SEF, no âmbito da prevenção e investigação de crimes relacionados com a imigração ilegal em que estejam envolvidas associações criminosas, seguem os termos previstos na Lei n.º 101/2001, de 25 de agosto.";

referências expressas a este órgão de polícia criminal, como as constantes nos artigos 4.º n.º 3 e 5.º n.º 2 do Regime Jurídico das Ações Encobertas.

Questões mais complexas surgem com a utilização de terceiros como agentes encobertos. Tal como refere Isabel Oneto, o Regime Jurídico das Ações Encobertas não define nem se debruça sobre a temática de quem pode ser o terceiro, quais os critérios para este ser selecionado e recrutado ou qual o tipo de controlo que será sobre ele efetuado, nomeadamente quando comparado com a supervisão exercida sobre o agente encoberto que seja funcionário de investigação criminal da Polícia Judiciária. Para a autora, não seria de estanhar que este órgão de polícia criminal oferecesse contrapartidas aos terceiros para que estes aceitassem participar nas ações encobertas, o que seria, de todo, ilegal, uma vez que o mesmo não dispõe de mecanismos legais para encetar este tipo de negociações[159]. Na mesma senda, Sandra Pereira alerta para o facto de poderem surgir, em relação à utilização de terceiros como agentes encobertos, situações de violação de preceitos constitucionais, porquanto, quando confrontados com o pedido, por parte da Polícia Judiciária, para atuar como agentes encobertos, os terceiros poderão aceitar o mesmo, mas não com plena liberdade na determinação da sua vontade, pela pressão policial exercida ou até mesmo a ameaça de início de procedimento criminal. Contudo, tal configura uma forma de coação moral, conhecido método proibido de prova, nos termos do disposto na alínea e) do n.º 2 do artigo 126.º do Código de Processo Penal[160].

De facto, parece-nos que o legislador, ao não especificar exaustivamente os mais pequenos aspetos deste regime jurídico, deixou espaço para lacunas que podem acabar por vir a ter grandes proporções, como é o caso da utilização de terceiros como agentes encobertos, sendo que, numa próxima alteração legislativa, deveria tal situação ser devidamente acautelada.

Sob a epígrafe *Âmbito de Aplicação*, o artigo 2.º do Regime Jurídico das Ações Encobertas apresenta um catálogo taxativo de crimes, cuja investigação criminal se pode efetuar por meio do recurso a uma ação encoberta. Verificou-se, com a consagração deste regime, um alargamento substancial do *numerus clausus* de crimes previsto na legislação anterior, o que, em última análise, poderá levar à banalidade da utilização deste método de obtenção de prova que, dado a limitação que opera a vários direitos fundamentais dos cidadãos, deveria cingir-se aos crimes que, de outro modo, dificilmente seriam descobertos[161]. Da mesma opinião partilha Rui Pereira, ao

[159] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, pp. 198-203.
[160] PEREIRA, Sandra, "A Recolha de Prova por Agente Infiltrado", In: *Prova Criminal e Direito de Defesa – Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal*, coordenação de Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, 2010, pp. 151-152.
[161] *Idem*, p. 149;

entender que "*Crimes irrepetíveis ou que se não insiram numa lógica de continuidade, relativamente aos quais se não formulam específicas exigências de prevenção, não justificam o recurso ao 'agente encoberto', mesmo que previstos o amplo catálogo do artigo 2.º.*"[162].

Não obstante, atualmente integram o catálogo de crimes no âmbito da investigação dos quais se pode recorrer às ações encobertas os seguintes: homicídio voluntário, desde que o agente não seja conhecido; 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; crimes relativos ao tráfico e viciação de veículos furtados ou roubados; escravidão, sequestro e rapto ou tomada de reféns; tráfico de pessoas; organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo; 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; crimes executados com bombas, granadas, matérias ou engenhos explosivos, armas de fogo e objetos armadilhados, armas nucleares, químicas ou radioativas; roubo em instituições de crédito, repartições da Fazenda Pública e correios; associações criminosas; crimes relativos ao tráfico de estupefacientes e de substâncias psicotrópicas; branqueamento de capitais, outros bens ou produtos; corrupção, peculato e participação económica em negócio e tráfico de influências; fraude na obtenção ou desvio de subsídio ou subvenção; infrações económico-financeiras cometidas de forma organizada ou com recurso à tecnologia informática; infrações económico-financeiras de dimensão internacional ou transnacional; contrafação de moeda, títulos de créditos, valores selados, selos e outros valores equiparados ou a respetiva passagem; e, por último, crimes relativos ao mercado de valores mobiliários.

Para que se possa recorrer ao emprego de um agente encoberto torna-se necessário o preenchimento dos requisitos plasmados no artigo 3.º do Regime Jurídico das Ações Encobertas, nomeadamente deve-se dar cumprimento a um princípio de adequação e de proporcionalidade. No que concerne ao princípio da adequação, o mesmo postula que a eficácia da ação encoberta deve ser adequada face às finalidades que se pretendem atingir com a mesma – trata-se de saber se a ação encoberta é imprescindível e insubstituível para a descoberta da verdade material. Por seu turno, o princípio da proporcionalidade determina que é necessário selecionar quais os casos

[162] PEREIRA, Rui, "O 'Agente Encoberto' na Ordem Jurídica Portuguesa", In: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, pp. 25-26.

em que os crimes em apreço cuja investigação criminal justifica levar a cabo ações encobertas; e compreender se nenhum dos outros meios de obtenção de prova legalmente previstos se afigura apto, adequado e suficiente para adquirir o material probatório que a ação encoberta revelará[163].

No entendimento de Isabel Oneto, o recurso às ações encobertas depende da verificação de dois pressupostos distintos, a saber: a existência de indícios sérios de que foi cometido ou está prestes a sê-lo um dos crimes previstos no catálogo do artigo 2.º do Regime Jurídico das Ações Encobertas; e os indícios em causa revelarem que os crimes em apreço se inserem no âmbito do terrorismo ou da criminalidade grave ou altamente violenta. Para a autora, após verificar-se o preenchimento destes requisitos, torna-se, ainda, necessário, dentro da própria ação encoberta, optar por aquela que se afigure menos gravosa, desde que cumpra a finalidade pretendida[164].

Além dos requisitos *supra* expostos, nos termos do disposto no n.º 3 do artigo 3.º do Regime Jurídico das Ações Encobertas, a realização de ação encoberta no âmbito do inquérito depende da prévia autorização do magistrado do Ministério Público competente para o efeito, sendo tal autorização obrigatoriamente comunicada ao juiz de instrução e é a mesmo considerada validada caso não seja proferido despacho de recusa nas 72 horas seguintes. Caso a ação encoberta decorra, pelo contrário, ainda antes de existir um inquérito criminal, é competente para autorização o juiz de instrução criminal, mediante proposta apresentada pelo Ministério Público, sendo que nesta hipótese se torna imprescindível que exista uma probabilidade preponderante de vir a ser aberto o respetivo inquérito.

Decorre do n.º 6 do artigo 3.º do Regime Jurídico das Ações Encobertas que "*A Polícia Judiciária fará o relato da intervenção do agente encoberto à autoridade judiciária competente no prazo máximo de quarenta e oito horas após o termo daquela*.". O relato descritivo da ação encoberta levada a cabo é, no entendimento de Isabel Oneto, um momento processual relevante para a aferição da conformidade da ação encoberta com a autorização concedida. Esta exigência de comunicação, à autoridade judiciária competente, dos atos praticados ao abrigo da referida autorização implica duas imposições: a vinculação do órgão de polícia criminal aos termos em que a autorização foi concedida; e a obrigação da autoridade judiciária competente de aferir a conformidade da ação encoberta[165].

---

[163] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, *Bruscamente... A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1ª edição, Rei dos Livros, 2010, pp. 124-125;

[164] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, pp. 187-188.

[165] *Idem*, p. 192;

Apesar de o relato em apreço poder ser essencial para a fiscalização da ação encoberta por parte da autoridade judiciária competente, a verdade é que o n.º 1 do artigo 4.º do Regime Jurídico das Ações Encobertas determina que o mesmo só deve ser junto aos autos quando se reputar indispensável em termos probatórios. Ora, tal pode suscitar problemas maiores, mormente no que respeita ao direito de defesa do arguido que, na grande maioria dos casos, não tem acesso ao mesmo ou sequer conhecimento da sua existência. Nesta senda, Paulo Pinto de Albuquerque entende que o agente encoberto tem um dever de relato, na medida em que deve munir a autoridade judiciária competente com os elementos necessários para proferir uma decisão atualizada acerca da adequação da diligência de prova em que se consubstancia a ação encoberta. Para o autor, apesar de a junção aos autos do competente relato apenas estar prevista para os casos de ações encobertas com a utilização de identidade fictícia, nada obsta a que o mesmo seja junto quando se reporte a ações encobertas em que não tenha sido utilizada uma identidade fictícia, nos termos do disposto no n.º 1 do artigo 275.º do Código de Processo Penal, quando o Ministério Público o entenda necessário para fins de inquérito[166] [167].

No que respeita ao valor do relato, a maioria da doutrina entende que o mesmo não possui qualquer valor probatório, uma vez que defender o contrário implicaria admitir uma violação do princípio da imediação, incito no n.º 1 do artigo 355.º do Código de Processo Penal. Nesta senda, entende Sandra Pereira que "*Por um lado, não faz sentido dizer que o relato não tem valor probatório quando a lei diz expressamente que ele será junto ao processo quando for indispensável em termos probatórios. (...) Mas, por outro lado, admitir que o relato do agente infiltrado sobre a ação encoberta tem algum valor probatório, é amputar em grande medida o sentido útil do princípio da imediação*.". Perfilhamos do entendimento da autora, quando refere que o relato do agente encoberto deve ser conjugado com o seu depoimento em sede de audiência de discussão e julgamento, determinando a conclusão de que o relato, por si só, não terá valor probatório, tal apenas acontecerá quando conjugado com outros meios de prova[168].

O depoimento do agente encoberto encontra-se previsto no n.º 3 do artigo 4.º do Regime Jurídico das Ações Encobertas, nos termos do qual a autoridade judiciária competente pode, mediante decisão fundamentada, oficiosamente ou a requerimento da Polícia Judiciária, autorizar que o agente encoberto que tenha atuado com identidade fictícia preste depoimento sob esta

[166] Vide artigo 275.º n.º 1 do Código de Processo Penal: "*1 - As diligências de prova realizadas no decurso do inquérito são reduzidas a auto, que pode ser redigido por súmula, salvo aquelas cuja documentação o Ministério Público entender desnecessário.*";

[167] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3ª edição atualizada, Universidade Católica Editora, 2009, p. 660.

[168] PEREIRA, Sandra, "A Recolha de Prova por Agente Infiltrado", In: *Prova Criminal e Direito de Defesa – Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal*, coordenação de Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, 2010, pp. 153-154.

identidade em processo relativo aos factos objeto da sua atuação. Na hipótese de o juiz determinar, por indispensabilidade da prova, a comparência em audiência de julgamento do agente encoberto, deverão ser observadas as disposições previstas na Lei n.º 93/99, também designada por Lei de Proteção de Testemunhas.

Nos termos do disposto no n.º 1 do artigo 19.º da Lei de Proteção de Testemunhas, para que o agente encoberto possa depor em audiência de discussão e julgamento, com ocultação da sua identidade, torna-se necessário seguir um determinado procedimento, denominado processo complementar de não revelação de identidade, previsto no artigo 18.º do referido diploma legal; e devem, ainda, estar reunidas todas as condições apresentadas no artigo 16.º do diploma em apreço.

Sendo o depoimento do agente encoberto realizado em anonimato, o mesmo levanta, desde logo, problemas de imediação e contraditório, na medida em que não há um contacto direto nem a possibilidade de contrainterrogar, fazendo com que o direito de defesa do arguido se veja seriamente limitado. Nesta senda, Paulo Pinto de Albuquerque defende que o regime estipulado pelo n.º 3 do artigo 4.º do Regime Jurídico das Ações Encobertas é manifestamente insuficiente, porquanto a decisão de proteção da identidade do agente encoberto é tomada sem dar garantia ao princípio do contraditório, ao contrário do que se prevê no artigo 18.º da Lei de Proteção de Testemunhas[169]. Entende o autor que "*(...) esta diferenciação entre o regime do agente encoberto e o das testemunhas a quem é concedida a medida de não revelação de identidade é objetivamente injustificada e desproporcional. Com efeito, viola o princípio da proporcionalidade que os requisitos da intervenção da testemunha previstos nos artigo 16.º a 18.º da Lei n.º 93/99 não sejam correspondentemente aplicáveis à intervenção do agente encoberto. Portanto, o artigo 4.º n.º 3, da Lei n.º 101/2001, é inconstitucional, por violar o artigo 32.º n.º 1 da CRP (...), ao*

[169] Vide artigo 18.º da Lei de Proteção de Testemunhas:
"*1 - Para apreciação do pedido de não revelação de identidade é organizado um processo complementar, secreto e urgente, em separado, ao qual apenas tem acesso o juiz de instrução e quem ele autorizar.*
2 - O juiz de instrução assegurará a guarda e a confidencialidade do processo complementar.
3 - O juiz de instrução solicita à Ordem dos Advogados a nomeação de advogado com perfil adequado para a representação dos interesses da defesa, com intervenção limitada ao processo complementar, e procede, oficiosamente ou a requerimento, às diligências que repute necessárias para apuramento dos pressupostos da concessão da medida.
4 - Antes de proferir decisão, o juiz de instrução convoca o Ministério Público e o representante da defesa para um debate oral e contraditório sobre os fundamentos do pedido.
5 - A decisão que concede a medida estabelece uma designação codificada à testemunha, pela qual passará a ser referenciada no processo. A designação é comunicada à autoridade judiciária com competência na fase em que o processo se encontre.
6 - O arguido que assumir essa qualidade nos termos do disposto no artigo 57.º do Código de Processo Penal, após a concessão da medida de não revelação de identidade a uma testemunha, tem o direito de requerer em seu benefício o debate previsto no n.º 4. É correspondentemente aplicável o disposto nos n.os 3 e 4.
7 - A medida é revogada pelo juiz de instrução, a requerimento do Ministério Público ou da testemunha, logo que se mostre desnecessária, realizadas as diligências convenientes e ouvido o Ministério Público, se não for o requerente.";

não reservar a um juiz a decisão aí referida e não prever qualquer forma de contraditório prévio a essa decisão."[170].

Cumpre, ainda, no que reporta ao depoimento do agente encoberto, referir que, de acordo com o n.º 2 do artigo 19.º da Lei de Proteção de Testemunhas, uma decisão condenatória a proferir não se pode fundar, exclusiva ou decisivamente, no depoimento de testemunhas cuja identidade não foi revelada. Torna-se necessário que tal meio de prova seja corroborado por outros, entendendo-se, assim, que o depoimento do agente encoberto se encontra subtraído à livre apreciação de prova por parte do julgador. Pelo contrário, em caso de proferimento de decisão absolutória, na ausência de disposição legal no mesmo sentido, entende-se que o princípio da livre apreciação de prova já vigorará em pleno[171].

Por último, o artigo 6.º do Regime Jurídico das Ações Encobertas regula a responsabilidade do agente encoberto pelos atos praticados precisamente no âmbito de uma ação encoberta. Dispõe o n.º 1 deste preceito legal 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.*".

Ora, no que diz respeito ao tipo de atos praticados pelo agente encoberto, a doutrina não é unânime. Com efeito, Isabel Oneto entende que os atos de execução de uma infração integram apenas o conceito de tentativa, nos termos do n.º 2 do artigo 22.º do Código Penal, pelo que estarão afastadas da previsão legal do artigo 6.º n.º 1 do Regime Jurídico das Ações Encobertas, as infrações consumadas[172] [173]. Numa tese contrária encontra-se Nuno Miguel Loureiro que, discordando de Isabel Oneto, aponta como argumentos o facto de os atos de execução, apesar de integrarem o conceito de tentativa, não se resumirem a estes; a questão de a cumplicidade ser efetivamente punida e esta implicar o começo da execução do crime pelo respetivo autor; e, ainda, o facto de um tal entendimento implicar uma restrição enorme à atuação do agente encoberto, o que seria desprovido de sentido, na medida em que se estaria a retirar uma enorme eficácia a um

---

[170] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3ª edição atualizada, Universidade Católica Editora, 2009, pp. 660-661;

[171] PEREIRA, Sandra, "A Recolha de Prova por Agente Infiltrado", In: *Prova Criminal e Direito de Defesa – Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal*, coordenação de Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, 2010, p. 158.

[172] Vide artigo 22.º n.º 2 do Código Penal:

"*2 - São atos de execução:*

a) Os que preencherem um elemento constitutivo de um tipo de crime;

b) Os que forem idóneos a produzir o resultado típico; ou

c) Os que, segundo a experiência comum e salvo circunstâncias imprevisíveis, forem de natureza a fazer esperar que se lhes sigam atos das espécies indicadas nas alíneas anteriores.";

[173] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, pp. 152-153;

método de obtenção de prova, a que se recorre precisamente pela extrema eficácia do mesmo[174]. Somos, nesta problemática, forçados a concordar com Nuno Miguel Loureiro, porquanto não nos parece que o espírito do legislador tenha sido restringir a atuação do agente infiltrado de tal modo que afetaria gravemente a efetividade da ação encoberta.

Mais unanimidade tem a doutrina apresentada relativamente ao modo de justificar a isenção de responsabilidade do agente encoberto, classificando a mesma como uma causa de exclusão de ilicitude estritamente penal[175]. Para que tal causa de exclusão de ilicitude possa operar, defende Nuno Miguel Loureiro ser necessário a verificação de vários pressupostos, a saber: a legalidade da ação encoberta; a prática de atos preparatórios ou de execução; a comparticipação; a proibição de instigação e da autoria mediata; e, por último, a proporcionalidade[176]. Por seu vez, no que toca a este último pressuposto, Rui Pereira defende que existem três critérios para a verificação da referida proporcionalidade, como sejam o facto de haver bens jurídicos cujo sacrifício não é razoável exigir; a superioridade dos bens jurídicos a salvaguardar em relação aos que se sacrificam; e o grau de perigo de continuação da atividade criminosa e a sua iminência[177].

Caso ocorra uma situação de excesso de atuação por parte do agente encoberto, em que este pratique outros atos que não os previstos no n.º 1 do artigo 6.º do Regime Jurídico das Ações Encobertas, a mesma será punível nos termos gerais, podendo este, contudo, beneficiar de uma atenuação especial, nos termos do disposto na alínea b) do n.º 2 do artigo 72.º do Código Penal.

2.4. Ações encobertas noutros ordenamentos jurídicos

O recurso a ações encobertas e, nesta senda, à utilização do agente encoberto traduz-se num método de obtenção de prova que ultrapassa fronteiras e é comum a quase todos os ordenamentos jurídicos existentes, cada um com as suas especificidades. Especificidades essas que iremos, de seguida, atentar, no que concerne ao regime jurídico das ações encobertas adotado em Espanha, França, Bélgica, Holanda, Alemanha, Reino Unido e Estados Unidos da América.

A introdução da figura do agente encoberto em Espanha surgiu com a Ley Orgánica n.º 5/1999, de 13 de Janeiro que veio aditar à Ley de Enjuiciamento Criminal os artigos 263bis e

[174] LOUREIRO, Nuno Miguel, "A Responsabilidade Penal do Agente Encoberto", *In Revista do Ministério Público*, Separata, n.º 142, Ano 36, 2015, pp. 100-101;
[175] PEREIRA, Rui, "O 'Agente Encoberto' na Ordem Jurídica Portuguesa", In: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, p. 31;
[176] LOUREIRO, Nuno Miguel, "A Responsabilidade Penal do Agente Encoberto", *In Revista do Ministério Público*, Separata, n.º 142, Ano 36, 2015, pp. 96-118;
[177] PEREIRA, Rui, "O 'Agente Encoberto' na Ordem Jurídica Portuguesa", In: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, pp. 36-37;

282.ºbis[178]. De acordo com este último, o juiz de instrução e o Ministério Público podem autorizar a realização de ações encobertas, no seio das quais podem ser atribuídas identidades fictícias a funcionários da *Policía Judicial*. Esta identidade é atribuída ao funcionário pelo *Ministerio del Interior*, pelo prazo máximo de seis meses, podendo este ser prorrogado por períodos de igual duração, e é conservada pelo respetivo funcionário quando seja chamado a testemunhar em audiência de discussão e julgamento. O agente encoberto está isento de responsabilidade criminal, desde que observe, na sua atuação, a devida proporcionalidade e a mesma não constituía provocação. Uma particularidade do regime espanhol consubstancia-se no facto de o juiz poder conceder autorização para que se obtenham imagens e se grave conversas que ocorram entre o agente encoberto e o indivíduo investigado, ainda que as mesmas ocorram no interior de um domicílio.

Apontando as diferenças entre o regime português e o regime espanhol, Adán Gonzalez-Castell realça o facto de, em Portugal, existir um diploma legal concreto e específico para a regulamentação das ações encobertas, ao passo que, em Espanha, existe apenas um fragmento da lei processual dedicada a esta temática. De igual modo, enquanto em Portugal podem desempenhar o papel de agentes encobertos tanto os funcionários de investigação criminal como terceiros, em Espanha tal papel encontra-se vedado aos funcionários de autoridade policial, categoria na qual se inserem todos os membros das forças e corpos de segurança. Em Espanha, o relato da ação encoberta é sempre junto aos autos na sua totalidade e a finalidade da ação

[178] Vide artigo 282.º bis da Ley de Enjuiciamento Criminal, disponível em https://bityli.com/adVYe, último acesso em 30-07-2021:
"*1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.*
La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad.
La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.
2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre.
Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.(...)
5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.
Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.";

encoberta prende-se só com a investigação de crimes que já tiveram lugar, inexistindo uma finalidade de prevenção[179].

Em França, as ações encobertas surgiram em 1991 quando seis funcionários alfandegários foram condenados pela prática do crime de tráfico de droga. Em sua defesa alegaram que se tinham infiltrado numa rede de tráfico de droga, que levou à apreensão de vários quilos de estupefacientes e à detenção dos traficantes. A condenação destes funcionários provocou uma revolta, tendo sido convocada uma greve geral na alfândega que provocou inúmeros prejuízos.

Atualmente, a atuação do agente encoberto encontra-se prevista na L. 627-7 § 2 do Código de Segurança Pública e no artigo 67bis do Código Aduaneiro, nos termos dos quais é permitido o recurso a esta figura para a investigação de crimes de tráfico de estupefacientes e precursores. Não obstante se exija uma autorização para a realização da ação encoberta, os procedimentos posteriores são deixados a cargo do agente encoberto, que determina quais os atos em concreto que praticará para obter a finalidade prevista. Este não é responsável penalmente, sendo proibida a provocação do crime. Nesta senda, a jurisprudência tem vindo a entender que os agentes encobertos podem levar ao cometimento do crime e não ser responsabilizados por isso, desde que provem que a intenção criminosa já existia no indivíduo investigado antes da sua intervenção. Aos informadores podem ser atribuídas recompensas, sejam estas monetárias ou em forma de redução de pena[180].

Na Bélgica, as ações encobertas encontram-se previstas em duas circulares emitidas pelo Ministério da Justiça, no âmbito das quais se estipula que só os oficiais da polícia podem ser agentes encobertos, sendo permitida a utilização de identidade fictícia. Os agentes encobertos não podem recorrer à provocação, não podem cometer crimes, exceto quando estritamente necessário e o princípio da proporcionalidade e subsidiariedade funcionam como limites da ação encoberta. Operam, ainda, uma distinção entre dois tipos de ações encobertas: as *sting operations* e as *flash roll*. Nas primeiras, o agente encoberto simula o seu interesse em comprar mercadoria, com base numa oferta de armas, droga, o que interessar ao suspeito; nas segundas, o agente encoberto encontra-se na posse de quantias avultadas em dinheiro, com o intuito de convencer a outra parte a vender determinada substância ilícita[181].

---

[179] GONZALEZ-CASTELL, Adán Carrizo, "El Agente Infiltrado en España y Portugual – Estudo Comparado a la Luz de las Garantias y de los Principios Constitucionales", In: Centro de Investigação do ISCPSI (Org.), *Criminalidade Organizada e Criminalidade de Massa – Interferências e Ingerências Mútuas,* coordenação de Manuel Monteiro Guedes Valente, Almedina, 2009, pp. 188-196;

[180] ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005, pp. 100-101;

[181] *Idem*, pp. 101-102;

No ordenamento jurídico holandês, o recurso às ações encobertas encontra-se limitado aos casos de criminalidade grave, sendo que o agente encoberto pode cometer crimes, mas deve sempre guardar respeito pelos princípios da subsidiariedade e da proporcionalidade. O acesso a este meio de obtenção de prova tem que ser especificamente fundamentado, o que normalmente acontece com a simples referência a informações provenientes dos serviços secretos de informação holandeses ou da Interpol. Admite-se o recurso a terceiros na qualidade de agente encoberto, exigindo-se, contudo, que os mesmos não possuam registo criminal e que tal só aconteça quando não seja possível recorrer a agentes de autoridade[182].

Na Alemanha, as ações encobertas surgiram com a aprovação da Lei contra o Tráfico Ilícito de Estupefacientes e Outras Manifestações de Criminalidade Organizada, de 22 de Setembro de 1992, só podendo apenas ser utilizadas nos casos em que os outros meios previstos não sejam suficientes e as investigações criminais ficam votadas ao insucesso. É necessário que existam indícios suficientes de que o crime cometido seja considerado grave, no domínio do tráfico de droga ou armas, falsificação de moeda, documento, valores, segurança do Estado ou que o mesmo tenha sido no âmbito da criminalidade organizada[183].

No Reino Unido, assistimos a uma inovação: a existência de um código de conduta do agente encoberto. As ações encobertas têm como objetivo a recolha de prova que permita o julgamento e condenação dos suspeitos, mas também são desenvolvidas no âmbito da prevenção e deteção de crimes. Têm um prazo máximo de três meses, podendo este ser renovado e a autorização para a mesma tem que ser reduzida a escrito. Em caso de urgência, a autorização pode ser oral e tem uma validade máxima de 72 horas[184].

Por último, os Estados Unidos da América estabeleceram uma prorrogativa de imunidade geral para todos os funcionários policiais que realizem ações encobertas. O Código Federal Americano regula a realização de ações encobertas no caso da prática de crimes de tráfico de droga e prevê o pagamento aos informadores, referindo que o dinheiro despendido para a compra de substâncias ilícitas é, posteriormente, reintegrado no orçamento da Administração, caso as mesmas venham a ser apreendidas[185]. Igualmente permitida é a criação de empresas fictícias no âmbito da investigação criminal e das ações encobertas.

Nesta senda, é extremamente conhecido o caso ABSCAM, no âmbito do qual, em 1978, foi criada pelo *Federal Bureau of Investigation* uma empresa fictícia, denominada de *Abdul*

[182] *Idem*, pp. 103-104.
[183] *Idem*, pp. 96-97;
[184] *Idem*, pp. 104-105;
[185] *Idem*, p. 105;

Enterprises, que fizeram acreditar ser detida por um *sheik* árabe que estava interessado em investir o dinheiro proveniente do negócio do petróleo em obras de arte. Foram recrutados vários informadores que colocaram os agentes do *Federal Bureau of Investigation* em contacto com criminosos para compra de arte e a investigação levou a vários políticos corruptos que se ofereceram para estabelecer contactos com congressistas americanos, com o intuito de dar asilo ao *sheik* nos Estados Unidos, mediante a promulgação de legislação privada e o pagamento de subornos. Acabaram por ser presos e condenados um senador, seis congressistas e mais de uma dúzia de criminosos e funcionários corruptos. Apesar de se ter gerado grande controvérsia acerca da legalidade da operação, os tribunais mantiveram todas as condenações[186].

Encontrando-se já delimitados todos os conceitos e especificidades relativas às ações encobertas, cumpre, de seguida, relacionar as mesmas com o plano digital e compreender como se desenrolam as investigações criminais neste plano.

[186] Cfr. síntese do caso apresentada pelo Federal Bureau of Investigation, disponível em https://bityli.com/6adkO, último acesso em 30-07-2021.

3. A LEI DO CIBERCRIME E AS AÇÕES ENCOBERTAS EM AMBIENTE DIGITAL

Temos vindo a assistir, nas últimas décadas, a uma enorme (r)evolução no que respeita às tecnologias de informação e comunicação, que acabaram por mudar, de forma fundamental, a vida em sociedade. Quer queiramos, quer não, as novas tecnologias acabam, mais tarde ou mais cedo, por se infiltrar em quase todos os aspetos das nossas vidas, criando oportunidades para melhorar determinadas capacidades já existentes. Com efeito, com o aparecimento da *internet*, foi possível observar várias mudanças, como sejam, no que toca às telecomunicações, a superação da telefonia clássica, frequentemente substituída pela troca de grandes quantidades de dados, em forma de voz, texto, música, imagens estáticas ou em movimento; troca esta que deixou, igualmente, de se efetuar apenas entre seres humanos, para, agora, ocorrer entre estes, entre seres humanos e computadores e, até, só entre computadores. O recurso ao e-mail passou a ser generalizado e a *internet* possibilitou, não só a facilidade de pesquisa, acesso e disseminação de informação, como também um aumento exponencial de informação e conhecimento disponível para todos[187].

Com a evolução das tecnologias, o fenómeno da Globalização começou, entre o final do século XX e início do século XXI, a ganhar cada vez mais forma e, atualmente, assistimos a um mundo onde as comunicações entre indivíduos e instituições são cada vez mais rápidas e fluídas, existe uma maior circulação de pessoas e bens, e as fronteiras físicas deixaram de ser um problema. Com o aparecimento de novas tecnologias e com a reinvenção e atualização das tecnologias já existentes, assistimos ao aparecimento da denominada Sociedade da Informação, no seio da qual, a informação encontra-se disponível para todos os cidadãos, de modo livre e aberto. Trata-se de "*(...) um verdadeiro modo de desenvolvimento económico e social baseado na aquisição, tratamento e difusão de informação por via das redes de comunicação digitais.*"[188]. Neste novo modelo de sociedade, a informação é a base de tudo e considerada uma ferramenta absolutamente indispensável para a construção do conhecimento de todos os indivíduos.

A drástica mudança da sociedade, operada pelo proliferação das novas tecnologias, teve um grande impacto na forma como os seres humanos se comportam e comunicam entre si. Atualmente, quase todos os cidadãos possuem um computador portátil, com ligação à *internet*,

[187] Neste sentido, vide Relatório Explicativo da Convenção sobre o Cibercrime, p. 1, disponível em https://bityli.com/x9pOB, último acesso em 05-08-2021;
[188] VERDELHO, Pedro, "Cibercrime", In: Associação Portuguesa do Direito Intelectual (Org.), *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003, p. 348;

têm várias contas de e-mail, para a sua vida profissional e pessoal, fazem compras online, lêem jornais em formato digital, em detrimento do formato físico – algo que, há apenas alguns anos atrás era impensável. O impacto que a tecnologia teve é especialmente visível nos mais jovens, que nunca experienciaram uma vida sem *internet* ou sem comunicações mediadas por um computador, por exemplo. São estes os casos em que a tecnologia moldou o comportamento dos indivíduos desde nascença, os denominados por Thomas Holt, Adam Bossler e Kathryn Seigfried-Spellar de *Digital Natives*, por oposição àqueles que nasceram num período temporal anterior ao aparecimento da *internet* e das tecnologias digitais e que tiveram, posteriormente que se adaptar às mesmas, os denominados *Digital Immigrants*[189].

Não obstante todas as vantagens já conhecidas que as novas tecnologias trouxeram, a verdade é que, à medida que estas foram avançando rapidamente, também a criminalidade organizada começou a tirar partido das mesmas. Na senda do ditado popular 'a oportunidade faz o ladrão', também o crime acompanhou todos avanços tecnológicos que foram ocorrendo e exploraram o mesmo, de modo a poder tirar o melhor partido disso. Como refere Jonathan Clough, "*The digital cameras and sharing photos on the Internet is exploited by child pornographers. The convenience of eletronic banking and online sales provides fertile ground for fraud. Eletronic communications such as email and SMS may be used to stalk and harass. The ease with which digital media may be shared has led to an explosion in copyright infringment.*"[190].

A maior facilidade na fluidez das comunicações, a existência de novos instrumentos para a prática de crimes já conhecidos, o aparecimento de novos tipos de crime em virtude da disponibilidade de novos instrumentos, geram aquilo a que Pedro Dias Venâncio apelida de *deslocação criminosa para a web*, porquanto um grande número de pessoas sente-se, agora, tentado a utilizar a *internet* para a prática de factos ilícitos que, sem tal ferramenta, nunca a tal se atreveriam. De igual modo, o autor fala numa *deslocação criminosa na web*, associando a tal o facto de, apesar de vários *sites* serem encerrados pelas autoridades, ser extremamente fácil transferir a informação que se pretende que não seja acedida, para outro site totalmente novo[191].

Por forma a justificar esta realidade da crescente atuação criminosa no ambiente digital, Paulo Santos, Ricardo Bessa e Carlos Pimentel indicam cinco fatores potenciadores, a saber: o custo reduzido dos bens tecnológicos; o custo reduzido de acesso à *internet*; a rápida expansão ocorrida no que respeita à banda larga; o aumento exponencial do conhecimento e do acesso, por

[189] HOLT, Thomas J., BOSSLER, Adam M., e SEIGFRIED-SPELLAR, Kathryn C., *Cybercrime and Digital Forensics – An Introduction*, Routledge, 2015, p. 2-4;
[190] CLOUGH, Jonathan, *Principles of Cybercrime*, Cambridge University Press, 2010, p. 3;
[191] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, 2001, p. 15.

parte dos meliantes, a meios de ocultação de provas digitais; e, por último, o crescimento da literacia computacional[192].

Já Jonathan Clough entende que o ambiente digital é um terreno extremamente fértil para a prática de ilícitos penais, identificando seis características das tecnologias digitais que, não só facilitam o crime, como prejudicam e dificultam a aplicação dos preceitos legais existentes.

A primeira destas características é a escala das novas tecnologias: a *internet*, em detrimento do ambiente físico e *offline*, permite aos seus utilizadores comunicarem com um grande número de indivíduos, de uma forma mais barata e mais fácil. Ora, esta quantidade enorme de utilizadores tem o seu lado negativo, porquanto funciona igualmente como um grande número de potenciais criminosos e vítimas, fazendo com que os crimes possam ser cometidos a uma escala nunca antes vista e totalmente inalcançável fora do ambiente digital. A segunda característica prende-se com a acessibilidade das tecnologias digitais. Atualmente, as novas tecnologias são cada vez mais omnipresentes e apresentam uma maior facilidade de uso. Em contraste com uma sociedade antiga, onde os computadores eram muito grandes, apenas utilizados pelos governos e instituições financeiras, nos dias de hoje, quase todos os cidadãos possuem acesso e conhecimento necessários para ter capacidade de cometer crimes *online*, e se não tiverem este conhecimento, podem facilmente adquiri-lo através de uma simples pesquisa na *internet*. Uma terceira característica que se pode identificar é o anonimato: com as novas tecnologias é possível esconder a verdadeira identidade de um indivíduo; tornar determinados dados confidenciais, através da encriptação; eliminar provas digitas com *softwares* simples que se encontram disponíveis, para todos, no mercado; ou até armazenar, deliberadamente, dados em servidores localizados em países onde a legislação vigente seja mais favorável. A portabilidade e transferibilidade é a quarta característica apontada pelo autor, na medida em que, atualmente, é possível armazenar uma enorme quantidade de dados num espaço bastante reduzido e proceder a uma réplica dos mesmos sem que, com tal atividade, ocorra uma qualquer diminuição da qualidade dos referidos dados. Como quinta característica, temos o alcance global das novas tecnologias: assim como é possível uma pessoa comunicar com outra que se encontre num continente completamente distinto, como se à sua beira se encontrasse, também os criminosos conseguem praticar factos ilícitos em qualquer posição do globo, desde que possuam uma conexão à *internet*. Por último, a sexta característica relaciona-se com a *absence of capable guardians*, isto é, o aparecimento das tecnologias digitais trouxe consigo vários desafios à efetiva

[192] SANTOS, Paulo, BESSA, Ricardo, e PIMENTEL, Carlos, *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, FCA, 2008, pp. 6-7.

aplicação da lei, o que faz com que não haja uma regulamentação eficaz do ambiente digital, provocando, por sua vez, um ecossistema apto à prática de crimes[193].

Face a todas as características apontadas e *supra* descritas, cumpre proceder a uma definição de criminalidade informática, também denominada de cibercriminalidade ou cibercrime, definição esta que, consoante os diversos autores, poderá ser mais ou menos abrangente. Lourenço Martins defende que o conceito de criminalidade informática se encontra delimitado pelos factos ilícitos que cumprem três requisitos, a saber: que tenham o computador por objeto; que usem o computador como instrumento específico da prática de crimes; e que o computador, enquanto instrumento, seja utilizado para violar direitos de personalidade[194]. Por seu turno, Pedro Dias Venâncio distingue entre a criminalidade informática em sentido amplo e em sentido estrito. Para o autor, "*Em sentido amplo, então, a criminalidade informática englobará toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios. Em sentido estrito, entenderemos nós que a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objeto de proteção.*"[195].

No presente capítulo, iremos tratar das especificidades dos crimes informáticos ou cibercrimes, analisando a legislação vigente, mormente a relativa à prova e à realização de ações encobertas em ambiente digital.

3.1. Evolução legislativa e a Lei do Cibercrime

Conforme já *supra* mencionado, o conceito de cibercrime poderá assumir um âmbito vasto e abrangente, sendo ainda um pouco controversa a exatidão deste termo; contudo, pretendemos, nesta sede, complementar um pouco mais as noções vindas de referir. Com efeito, Joshua B. Hill e Nancy E. Marion entendem que o termo cibercrime refere-se a "*(...) acts that involve criminal uses of the Internet or other networked systems to cause harm to others or some form of a disturbance. In short, the term 'cybercrime' refers to methods by which computers or other electronic devices are used to carry out criminal activity and cause harm to others*"[196]. Por seu

[193] CLOUGH, Jonathan, *Principles of Cybercrime*, Cambridge University Press, 2010, pp. 5-8;
[194] MARTINS, A. G. Lourenço, "Criminalidade Informática", In: Associação Portuguesa do Direito Intelectual (Org.), *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003, p. 12;
[195] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, 2001, p. 17.
[196] HILL, Joshua B., e MARION, Nancy E., *Introduction to Cybercrime – Computer Crimes, Laws and Policing in the 21st Century*, PSI Textbook, 2016, p. 5;

turno, e de modo a clarificar quaisquer dúvidas, a Comissão Europeia veio, num ato de comunicação ao Parlamento Europeu, ao Conselho e ao Comité das Regiões, denominado de *Rumo a uma política geral de luta contra o cibercrime*, esclarecer que deverá entender-se por cibercrime qualquer ato criminoso praticado através da utilização de redes de comunicação eletrónicas e sistemas de informação ou contra estas redes e sistemas. No entender da Comissão Europeia, deverá operar-se uma divisão no que toca às diferentes formas que o cibercrime pode adotar, a saber: formas tradicionais da atividade criminosa (crimes já existentes anteriormente mas que agora ocorrem por meio da *internet*, nos quais se inserem a usurpação de identidade e o *phishing*); publicação de conteúdo ilícito (como seja material de incentivo ao terrorismo, racismo, xenofobia ou abuso sexual de menores); e crimes referentes exclusivamente a redes eletrónicas (tratam-se de crimes novos, que até ao aparecimento da *internet* não eram conhecidos)[197].

No que respeita à natureza do cibercrime, Pedro Dias Venâncio defende que a informática desempenha um papel essencial no âmbito do mesmo e, bem assim, o cibercrime poderá, consoante a função desta, apresentar duas naturezas: uma em que a informática é um meio para a prática de crimes, e outra em que esta se apresenta como um elemento integrador do tipo legal de crime. Quando a informática é utilizada como um meio para a prática de crimes, estamos perante situação em que as tecnologias de informação e comunicação são aplicadas para praticar factos ilícitos próprios da realidade física, isto é, cujo tipo legal se encontra previsto de tal modo que a componente informática não é considerada como elemento integrador do crime. Por outro lado, a partir de dado momento, o Estado passou a entender que, dada a crescente inovação tecnológica, determinados produtos informáticos mereceriam uma proteção jurídica equivalente à existente em relação aos bens corpóreos e foi nessa altura que a informática começou a aparecer como elemento integrador do tipo legal de crime, ou seja, casos em que os elementos caracterizadores do tipo legal integram realidades informáticas[198].

Pedro Verdelho, por sua vez, opta por fazer uma distinção do cibercrime em três diferentes grupos: crimes que recorrem a meios informáticos, crimes referentes à proteção de dados pessoais e crimes informáticos propriamente ditos. Os crimes que recorrem a meios informáticos são aqueles que, tal como resulta da lei, só podem ser praticados por via do recurso a meios informáticos; contudo, tal característica em nada os distingue de crimes idênticos praticados com recurso a outros métodos. Apesar de o meio informático ser essencial, é possível a prática dos

[197] Vide Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões: Rumo a uma política geral de luta contra o cibercrime, disponível em https://bityli.com/q9Zi9, último acesso em 10-08-2021;
[198] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, 2001, pp. 18-21.

mesmos crimes, mas no ambiente físico, como é o caso da burla informática, burla nas comunicações e devassa por meio da informática, crimes previstos respetivamente nos artigos 221.º n.º 1, 221.º n.º 2 e 193.º, todos do Código Penal. Já os crimes referentes à proteção de dados pessoais correspondem a uma categoria tradicional de cibercrimes, no âmbito dos quais os bens jurídicos protegidos são a transparência na utilização da informática, a reserva da vida privada e o respeito pelos direitos, liberdades e garantias dos cidadãos; é o caso do acesso indevido, da viciação ou destruição de dados pessoais e da violação do dever de sigilo, previstos respetivamente nos artigos 47.º, 49.º e 51.º da Lei n.º 58/2019, de 08 de Agosto, denominada de Lei da Proteção de Dados Pessoais[199]. Por último, os crimes informáticos propriamente ditos englobam os crimes informáticos clássicos, normalmente dirigidos à proteção da integridade e disponibilidade dos sistemas e programas informáticos e os que anteriormente se encontravam previstos na Lei da Criminalidade Informática, revogada pela atual Lei do Cibercrime. Trata-se, a título de exemplo, dos crimes de falsidade informática, sabotagem informática, acesso ilegítimo e reprodução ilegítima de programa, respetivamente previstos nos artigos 3.º, 5.º, 6.º e 8.º da Lei do Cibercrime[200].

Relativamente à tipologia de crimes que integram o conceito de cibercrime, Joshua B. Hill e Nancy E. Marion defendem que o *sexting* (atividade de enviar fotos de pessoas menores de 18 anos nuas a outrem através do telemóvel), a usurpação de identidade (quando alguém obtém e usa ilicitamente os dados de outrem para obter uma vantagem patrimonial), o *hacking* (acesso ilegal a sistemas de computadores), o *cyberstalking* (quando os criminosos seguem constantemente a localização de determinada vítima e dão a essa pessoa uma sucessiva e não solicitada atenção) e o *phishing* (atividade de enviar e-mails para utilizadores com a intenção de obter a sua informação pessoal e privada para depois praticar outros crimes), entre outros, integram a categoria de crimes cometidos contra pessoas. Já nos crimes cometidos contra a propriedade, podemos encontrar os vírus (qualquer *software* malicioso que, uma vez instalado num computador, pode afetar o tráfego da rede ou perturbar o normal funcionamento do mesmo, como causar danos nas definições do sistema, apagar informações ou desativar sistemas de segurança), o *spyware* (*software* ou tecnologia que espia secretamente a atividade de um utilizador no computador e recolhe informação acerca de tal utilização) e o *ransomware* (*software* que impede o acesso a ficheiros por parte do utilizador, sendo estes posteriormente contactados a

[199] Disponível em https://bityli.com/LaRse, último acesso em 10-08-2021;
[200] VERDELHO, Pedro, "Cibercrime", In: Associação Portuguesa do Direito Intelectual (Org.), *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003, pp. 355-367.

informar que os seus ficheiros foram roubados ou encriptados e que se os quiserem de volta, terão de pagar o respetivo resgate), entre outros. Por último, na categoria dos crimes contra governos, temos o ciberterrorismo (qualquer ataque de motivação política contra sistemas de computador, programas ou dados informáticos que resultam numa violência extrema contra determinados alvos) e a *cyberwarfare* (capacidade de fazer grandes ataques a computadores, sites ou redes)[201].

Face às características das novas tecnologias e aos tipos de crime cometidos através da utilização de meios informáticos, dúvidas não restam relativamente à dificuldade existente para combater o fenómeno do cibercrime. Não obstante, desde cedo, foi apanágio do legislador, nacional e supranacional, tutelar juridicamente os bens contra os quais atentam os crimes que integram a noção de cibercrime. Foi em 1982 que surgiu, no Código Penal, a primeira referência à criminalidade informática, por meio do artigo 181.º, sob a epígrafe *Devassa por Meio da Informática*, que incriminava a criação, manutenção ou utilização de ficheiro automatizado de direitos informáticos[202]. Com a revisão de 1995, o conteúdo da referida norma legal passou para o artigo 193.º, sob a mesma epígrafe, com a alteração da moldura penal para pena de prisão até dois anos ou pena de multa até 240 dias. No que concerne a esta alteração, Lourenço Martins entende que a inserção desta norma não deveria ter ocorrido no Código Penal, mas sim na Lei da Proteção de Dados Pessoais, porquanto é "*(...) indesejável esta dispersão de normas criminais sobre o mesmo tema, levando ao seu desconhecimento pelos destinatários e a dificuldades de aplicação.*"[203].

Apesar de, como vimos, o Código Penal ter inicialmente previsto crimes praticados especificamente através de meios informáticos, só com a entrada em vigor da Lei n.º 109/91, de 17 de Agosto, denominada de Lei da Criminalidade Informática, se completou, de uma forma muito mais extensiva, esta realidade informática na criminalidade. A Lei da Criminalidade Informática[204] surgiu no seguimento da Recomendação n.º R (89) 9 do Conselho da Europa, sobre a criminalidade informática, onde era recomendado aos Estados que, caso pretendessem legislar

---

[201] HILL, Joshua B., e MARION, Nancy E., *Introduction to Cybercrime – Computer Crimes, Laws and Policing in the 21st Century*, PSI Textbook, 2016, pp. 58-83;

[202] Vide artigo 181.º do Código Penal de 1982, disponível em https://bityli.com/fWulB, último acesso em 10-08-2021:
"*1 - Será punido com prisão até 1 ano e multa até 60 dias quem:*
a) Criar ou mantiver um ficheiro automatizado de dados de carácter pessoal, em infração à lei;
b) Fornecer falsas informações no pedido de autorização de constituição ou manutenção de um ficheiro automatizado de dados de carácter pessoal ou proceder a alterações não consentidas pelo instrumento de criação;
c) Modificar, suprimir ou acrescentar de forma indevida informações pessoais a um ficheiro automatizado de dados de carácter pessoal;
d) Desviar da finalidade legalmente consentida informações de carácter pessoal não públicas.
2 - É punido com prisão até 2 anos quem processar ou mandar processar dados de carácter pessoal referentes a convicções políticas, religiosas, filosóficas, bem como outras atinentes à privacidade, em infração à lei.";

[203] MARTINS, A. G. Lourenço, "Criminalidade Informática", In: Associação Portuguesa do Direito Intelectual (Org.), *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003, pp. 18-19;

[204] Disponível em https://bityli.com/5X7gq, último acesso em 10-08-2021.

na matéria da cibercriminalidade, deveriam ter em conta os princípios diretores constantes da mesma. Tais princípios dividiam-se em duas listas diferentes: uma mínima e uma facultativa. A lista mínima traduzia-se no conjunto de factos ilícitos que deveriam fazer, obrigatoriamente, parte de uma qualquer lei relativa à criminalidade informática e que foram consagrados nos artigos 4.º a 9.º da Lei da Criminalidade Informática[205].

Num plano supranacional, posteriormente à emanação da Recomendação n.º R (89) 9 do Conselho da Europa, vários anos se passaram até que o assunto da criminalidade informática fosse novamente abordado, sendo que tal apenas aconteceu com a Recomendação n.º R (95) 13, do Conselho da Europa, que previa a necessidade de celebração de acordos internacionais que definissem a extensão da admissibilidade da pesquisa e apreensão de dados transnacionais. No seguimento de tal recomendação, o Comité Europeu para os Problemas Criminais do Conselho da Europa criou um comité próprio e autónomo de especialistas em cibercriminalidade, no seio do qual surgiu a Convenção n.º 185, de 23 de Novembro de 2001, em Budapeste, denominada de Convenção sobre o Cibercrime do Conselho da Europa. Tendo entrado em vigor a 01-07-2004, a Convenção sobre o Cibercrime foi o primeiro grande trabalho jurídico e normativo sobre o crime no ciberespaço[206].

A Convenção do Cibercrime[207], que se divide em quatro capítulos – utilização de terminologia, medidas a empreender a nível nacional: direito substantivo e direito processual, cooperação internacional e disposições final – apresenta três distintos objetivos: harmonizar as disposições penais substantivas a nível nacional e as disposições conexas na área da cibercriminalidade; dotar, no âmbito do código de processo penal de cada país, as autoridade encarregues da investigação criminal dos poderes necessários para investigar e iniciar procedimento criminal relativamente às infrações previstas na Convenção, assim como as cometidas por via de sistema informático ou, ainda, às provas eletrónicas; e implementar um regime rápido e eficaz a nível de cooperação internacional[208].

Em comparação com a Lei da Criminalidade Informática, à data vigente no ordenamento jurídico português, podemos verificar que as soluções previstas na Convenção já se encontravam, na sua grande maioria, previstas em Portugal. Contudo, a Convenção sobre o Cibercrime foi mais longe: previu mais definições ou alargou o âmbito de definições já existentes na Lei da Criminalidade Informática e estipulou novos tipos de crime ou procedeu a ajustes quanto aos

[205] VERDELHO, Pedro, BRAVO, Rogério, e ROCHA, Manuel Lopes, *Leis do Cibercrime*, Vol. I, Centro Atlântico, 2003, pp. 247-248;
[206] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, pp. 67-70;
[207] Disponível em https://bityli.com/6mJa4, último acesso em 10-08-2021;
[208] Vide ponto 16 do Relatório Explicativo da Convenção do Cibercrime, disponível em https://bityli.com/x9pOB, último acesso em 10-08-2021;

crimes já legalmente previstos. No que respeita à Convenção, cumpre, ainda, referir que se encontra previsto, no seu artigo 14.º, o âmbito de aplicação das medidas processuais consagradas, sendo permitido a cada Estado signatário, nos termos do disposto no n.º 3, formular reservas, o que sucedeu no caso de Portugal, que formulou uma reserva ao n.º 5 do artigo 24.º[209].

Posteriormente ao surgimento da Convenção sobre o Cibercrime, o Conselho da Europa emanou a Decisão-Quadro 2005/222/JAI, de 24 de Fevereiro, relativa a ataques contra sistemas de informação[210]. Ao tipificar vários tipos de ataques possíveis a sistemas informativos, a Decisão-Quadro veio completar o trabalho até então realizado pelas organizações internacionais e proporcionou o aparecimento, em Portugal, da Lei n.º 109/2009, de 15 de Setembro, denominada de Lei do Cibercrime. A Lei do Cibercrime, que veio transpor para a ordem jurídica portuguesa, a *supra* mencionada Decisão-Quadro e a Convenção sobre o Cibercrime, teve origem na Proposta de Lei n.º 289/X/4.ª, na Exposição de Motivos da qual se pode ler que "*Todas as atividades das sociedades modernas e das economias usam a Internet para seu apoio. Neste contexto, foi natural o surgimento de atividades ilegais associadas às redes de comunicação, usando-as e explorando as suas vulnerabilidades, criando assim riscos para a utilização quotidiana dos meios informáticos. Portugal tem, desde 1991, por impulso da recomendação R (89) 9 do Conselho da Europa, um quadro normativo que visa punir aquilo a que chamou os crimes informáticos: a Lei n.º 109/91, de 17 de Agosto. Este diploma, adequado à realidade que se destinava a regular na data em que entrou em vigor, pelo decurso de quase duas décadas, tornou-se deficitário.*"[211].

Como novidades relativamente à Lei da Criminalidade Informática, podemos observar a existência, no artigo 2.º da Lei do Cibercrime, de novos conceitos, como o de *sistema informático* e a melhoria de outros já existentes; assim como a consagração, no artigo 9.º do referido diploma legal, da responsabilidade das pessoas coletivas quanto aos factos ilícitos previstos nos artigos 3.º e seguintes, nos mesmos termos em que o são no âmbito dos crimes previstos no Código Penal.

---

[209] Aquando da ratificação, Portugal formulou a seguinte reserva, disponível em https://bityli.com/oBjfp, último acesso em 10-08-2021:
"*Portugal não concederá a extradição de pessoas:*
a) Que devam ser julgadas por um tribunal de exceção ou cumprir uma pena decretada por um tribunal dessa natureza;
b) Quando se prove que são sujeitas a processo que não oferece garantias jurídicas de um procedimento penal que respeite as condições internacionalmente reconhecidas como indispensáveis à salvaguarda dos 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.
Portugal só autoriza o trânsito em território nacional de pessoa que se encontre nas condições em que a sua extradição possa ser concedida.";
[210] Disponível em https://bityli.com/gygs6, último acesso em 10-08-2021;
[211] Vide Exposição de Motivos da Proposta de Lei n.º 289/X/4.ª, disponível em https://bityli.com/530zv, último acesso em 10-08-2021.

Quanto aos factos ilícitos presentes da Lei do Cibercrime, os artigos 3.º a 8.º prevêem os crimes de falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido. Já quanto às disposições processuais, mais relevantes para o estudo em apreço, com a entrada em vigor da Lei do Cibercrime assistimos a uma verdadeira inovação, tendo sido criadas novas normas com o intuito de serem aplicadas às investigações criminais. Como meios aplicáveis a estas investigações temos, assim, na Lei do Cibercrime, a preservação expedita de dados, a revelação expedita de dados de tráfego, a injunção para apresentação ou concessão do acesso a dados, a pesquisa de dados informáticos, a apreensão de dados informáticos, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, a interceção de comunicações e as ações encobertas em ambiente digital. No âmbito do artigo 11.º, entendeu o legislador que os novos meios de investigação criminal se aplicariam a processos relativos a crimes previstos nos artigos 3.º a 8.º, aos cometidos por meio de um sistema informático e àqueles em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, com exceção nos artigos 18.º e 19.º do diploma legal em apreço.

A preservação expedita de dados encontra-se prevista no artigo 12.º da Lei do Cibercrime. De acordo com o n.º 1 deste preceito legal "*Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa*.". Esta preservação poderá também ser ordenada pelo órgão de polícia criminal competente, desde que para tal obtenha a necessária autorização por parte da autoridade judiciária competente, ou quando esteja perante uma situação de urgência ou perigo na demora. Nos termos do disposto no n.º 3 do artigo 12.º da Lei do Cibercrime, a ordem de preservação deve conter a discriminação da natureza dos dados; a sua origem e destino, se forem conhecidos; e o período de tempo pelo qual deverão ser preservados, até um máximo de três meses. No que respeita a este período temporal, Benjamim Silva Rodrigues entende que o mesmo não deverá ser ultrapassado, sendo vedada, assim, a possibilidade de renovação, tal como ocorre no caso das escutas telefónicas. Apesar de este ser o seu entendimento, reconhece que, tendo em conta o prazo absoluto de conservação de dados previsto

no artigo 6.º da Lei n.º 32/3008 de um ano, poderão surgir casos em que tal renovação ocorra ao abrigo do disposto no n.º 5 do artigo 12.º da Lei do Cibercrime[212].

O artigo 13.º da Lei do Cibercrime prevê a revelação expedita de dados de tráfego, no âmbito da qual, com o intuito de assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo 12.º da Lei do Cibercrime, indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada, independentemente do número de fornecedores de serviço que nela participaram.

Por seu turno, a injunção para apresentação ou concessão do acesso a dados encontra-se prevista no artigo 14.º da Lei do Cibercrime, de acordo com o qual, caso seja necessário à produção de prova, no âmbito de um procedimento criminal, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. Será punido por desobediência quem, tendo sido interpelado pela autoridade judiciária competente, não permitir o acesso aos dados requeridos, nos termos do disposto no n.º 3 do artigo 14.º da Lei do Cibercrime. Cumpre salientar que, de acordo com os n.º 5 e 6 do preceito legal em estudo, esta medida não poderá ser dirigida ao suspeito ou arguido, assim como tal não poderá ocorrer quanto aos sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista, na senda do respeito pelo segredo profissional.

A pesquisa de dados informáticos encontra-se prevista no artigo 15.º da Lei do Cibercrime, de acordo com o qual "*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.*". A referida autorização tem um prazo máximo de 30 dias e a pesquisa de dados informáticos poderá realizar-se com a ausência da mesma, pelos órgãos de polícia criminal, quando a pesquisa for voluntariamente consentida por quem tiver a

[212] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV, *Da Prova Eletrónico-Digital e da Criminalidade Informática*, 1ª edição, Rei dos Livros, 2011, p. 522.

disponibilidade ou controlo desses dados e quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa, nos casos de terrorismo, criminalidade violenta ou altamente organizada.

A apreensão de dados informáticos, por sua vez, encontra-se regulamentada no artigo 16.º da Lei do Cibercrime, sendo que quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

O artigo 17.º da Lei do Cibercrime prevê a medida de apreensão de correio eletrónico e registos de comunicações de natureza semelhante, nos termos da qual quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

A interceção de comunicações aparece prevista no artigo 18.º da Lei do Cibercrime, sendo admissível o recurso à interceção de comunicações em processos relativos a crimes previstos na Lei do Cibercrime ou cometidos por meio de um 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 Código de Processo Penal. De salientar é que, nos termos do n.º 2 do artigo 18.º, a interceção de comunicações apenas pode ter lugar no âmbito de um inquérito, isto é, quando já decorre um procedimento criminal, não podendo ocorrer no âmbito de uma qualquer ação preventiva.

Por último, o artigo 19.º da Lei do Cibercrime prevê as ações encobertas em ambiente digital, dispondo no n.º 1 que "*É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes: a) Os previstos na presente lei; b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla*

qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.". Já o n.º 2 determina que, sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações. Quanto ao regime jurídico previsto para este método oculto de investigação criminal, alvo principal do presente estudo, ou falta do mesmo, teceremos *infra* os necessários e esclarecedores comentários.

3.2. Investigação criminal em ambiente digital

A investigação criminal, enquanto atividade de recolha de elementos de prova que é, tem como objetivo último a descoberta da verdade material no âmbito de um determinado processo penal – pretende-se compreender se existe, efetivamente, a prática de um crime, quando e onde teve o mesmo lugar, quem foi o seu autor e no âmbito de que circunstâncias foi o mesmo praticado. Assim, conforme entende Pedro Verdelho, o objeto da investigação criminal é "*(...) descobrir culpados da prática de crimes (...) e preparar elementos de prova que possam vir a ser reproduzidos em julgamento de forma a permitir ao tribunal decidir o concreto grau de culpabilidade daqueles a quem lhe compete julgar.*"[213].

Com o aparecimento da *internet* e das consequentes novas tecnologias, a investigação criminal, que se encontrava voltada para os aspetos da realidade física, teve, necessariamente, que se adaptar e reinventar para poder combater, de forma eficaz, a criminalidade que tirou partido de tais inovações tecnológicas para deslocar o seu plano de atuação para o ambiente digital. A prática de crimes em ambiente digital veio suscitar desafios e problemas à atividade de recolha de prova, porquanto a mesma passou agora a possuir características próprias e um formato digital.

Com o intuito de delimitar o conceito de prova digital, Eoghan Casey define-a como "*(...) any data stored or transmitted using a computer that support or refute a theory of how an offense occurred*

or that address critical elements of the offense such as intent or alibi.", assumindo estes dados a forma de várias combinações de números que, em *ultima ratio*, representam as mais variadas informações, como texto, imagens, áudio e vídeo. Para o autor, as provas digitais são de tal modo omnipresentes que é raro o crime praticado que não possua dados associados que, por sua vez,

[213] VERDELHO, Pedro, "A Obtenção de Prova no Ambiente Digital", In: *Revista do Ministério Público*, n.º 99, Ano 25, Jul/Set 2004, p. 117, disponível em https://bityli.com/M6tnJ, último acesso em 11-08-2021.

se encontram armazenados em sistemas de computadores[214]. Enquanto o Scientific Working Group on Digital Evidence entende que a prova digital se traduz em "*Information of probative value stored or trasmitted in digital form*"[215]; Benjamim Silva Rodrigues vai mais longe e define-a como "*(...) qualquer tipo de informação, com valor probatório, armazenada [em repositório eletrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou rede de comunicações eletrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital.*"[216].

Não obstante as definições *supra* apresentadas, que resultam inteiramente da doutrina, é possível constatar, através de uma detalhada análise à diversa legislação portuguesa em matéria de prova no âmbito do processo penal, que o legislador não procurou apresentar uma qualquer definição para a prova digital, tendo optado, antes, por utilizar dispersamente e sem critério diversas expressões nesse âmbito – como sejam os exemplos das expressões *guardada em suporte digital*, prevista no artigo 189.º do Código de Processo Penal, ou *prova em suporte eletrónico*, previsto nos artigos 1.º, 11.º n.º 1 c), 18.º n.º 1 b) e 20.º, todos da Lei do Cibercrime[217]. Ora, dado o papel, cada vez maior, desempenhado pela cibercriminalidade no âmbito da criminalidade organizada, e não só, parece-nos bastante infeliz que o legislador não tenha, ainda, adotado uma qualquer definição de prova digital e, bem assim, que não tenha optado por elaborar um regime jurídico onde a existência e recolha da mesma fosse exaustivamente regulamentada, para acautelar, não só os interesses das investigações criminais, como, de igual modo, os direitos e garantias dos cidadãos.

Tendo em conta as particularidades da prova digital e as suas especificidades, cumpre atentar nas diversas características da mesma. Benjamim Silva Rodrigues identifica, à semelhança de outros autores, sete características da prova digital, a saber: efemeridade; fragilidade e fácil alterabilidade; volatilidade e instabilidade; aparente imaterialidade e invisibilidade; complexidade; dispersão e disseminação; e dinamismo e mutabilidade.

A efemeridade, precariedade ou não durabilidade da prova digital traduz-se no facto de, por vezes, a mesma não ficar disponível por tempo suficiente para poder ser armazenada num determinado dispositivo, com o intuito de poder ser acedida sempre que necessário. Já a característica da fragilidade ou fácil alterabilidade diz respeito à problemática de, quando se pretende aceder e recolher prova digital, ser elevada a probabilidade de se proceder a alterações

---

[214] CASEY, Eoghan, *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, 3ª edição, Elsevier Inc. All, 2011, disponível em https://bityli.com/r8m8h, último acesso em 12-08-2021, p. 7;
[215] Vide informação disponível em https://www.swgde.org/;
[216] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade Informática*, 1ª edição, Rei dos Livros, 2011, p. 39;
[217] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 99.

na mesma – daí que seja necessário que o investigador faça uma precisa identificação do tipo de prova digital em causa e garanta a sua inalterabilidade antes de proceder à sua recolha. A prova digital pode, num primeiro momento, apresentar umas determinadas características, e num segundo, apresentar já uma natureza totalmente diferente que afeta diretamente a possibilidade da sua recolha, e assim o é porque a mesma é dotada de uma volatilidade e instabilidade enorme. De igual modo, a imaterialidade ou não visibilidade características da prova digital requerem que a pessoa encarregue de a identificar e recolher tenha especiais capacidades técnicas, caso contrário poderá levar a uma situação onde a prova se perde ou altera, o que fará com que a sua força probatória seja inválida em juízo. Estas especiais capacidades técnicas são necessárias na medida em que, na grande maioria dos casos, a recolha de prova digital implica o acesso a sistemas e redes informáticas e o conhecimento de chaves de desencriptação, dado a mesma ser complexa e codificada. A prova digital é, também, dispersa e difusa porquanto se espalha pelos mais variados terminais, computadores e redes que se estendem por uma grande área geográfica, motivo pelo qual a cibercriminalidade é, também ela, alheia a fronteiras físicas. Por último, a característica do dinamismo e mutabilidade da prova digital prende-se com o facto de a mesma assumir um papel dinâmico no sistema informático, cabendo ao investigador comparar diversos períodos temporais para poder aceder à prova que se afigure favorável para o crime que se encontra a investigar[218].

Uma breve análise das características *supra* mencionadas é suficiente para compreender a clara distinção entre a realização de uma investigação criminal em ambiente físico e uma investigação criminal em ambiente digital, que implica necessariamente a recolha de prova digital. Orin Kerr demonstra, de forma bastante tangível e elucidativa, esta distinção com o simples exemplo de um roubo a um banco. Um determinado indivíduo decide conduzir, no seu carro, até a um banco, onde entra e discretamente entrega à funcionária que se encontrava a atendê-lo ao balcão um papel, onde se pode ler "*Isto é um assalto. Entregue-me o dinheiro e ninguém se magoa*.". A funcionária, observando a arma escondida no casaco do indivíduo, entrega-lhe todo o dinheiro num saco, que este pega e foge. Com este já no exterior, a funcionária chama a polícia. Para a investigação criminal da prática deste crime, o inspetor da polícia vai começar por recolher os depoimentos das testemunhas, pedindo que descrevam o que aconteceu e traços físicos do indivíduo; e recolhe provas físicas que têm como objetivo ajudar a relacionar a prática do crime

[218] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade Informática*, 1ª edição, Rei dos Livros, 2011, pp. 41-44.

com o indivíduo, como sejam impressões digitais deixadas no papel entregue à funcionária do banco ou até alguma marca de caligrafia distinta no mesmo. Numa outra situação, o mesmo indivíduo decide levar a cabo um furto ao mesmo banco, mas desta vez, pretende fazê-lo a partir do conforto de sua casa e do seu computador conectando-se à *internet* através de uma conta que possui com um provedor local de serviços de *internet* (*Internet Service Provider*). Não obstante o seu objetivo seja obter acesso aos servidores do banco, o indivíduo utiliza vários computadores intermediários, até chegar efetivamente ao do banco. Quando consegue acesso ao computador do banco, cria uma conta bancária nova e dá instruções ao mesmo para considerar que a conta possui uma avultada quantia de dinheiro, sendo que, posteriormente, transfere esse dinheiro para uma conta *offshore*, impossível de rastrear. No dia seguinte, ao chegar ao trabalho, o funcionário do banco apercebe-se da situação e chama a polícia. Para a investigação criminal da prática deste crime, Orin Kerr salienta que não existem testemunhas no banco ou quaisquer provas físicas, apenas existem provas digitais e recolher as mesmas implica recolher e analisar toda a informação que possa ter ficado no computador do indivíduo criminoso. Tais informações são, por norma, muito escassas, apenas indicam que uma determinada pessoa, em qualquer ponto do globo, entrou no sistema informático do banco. Nestes casos, a melhor pista a que investigação criminal pode chegar é a descoberta do endereço de IP (*Internet Protocol*) registado nos servidores do banco. Este endereço identifica o computador que comunicou com os servidores do banco e, para encontrar o indivíduo, o inspetor terá que começar com este endereço de IP e seguir o *trail of electronic bread crumbs* até chegar ao computador de casa do indivíduo criminoso. Se for possível encontrar e analisar este computador, muito provavelmente será possível encontrar no mesmo provas contundentes[219].

Com este simples exemplo, o autor pretende demonstrar as evidentes diferenças entre a prática de crimes e a consequente investigação criminal no âmbito físico e no ambiente digital, diferenças estas que justificam a existência de um regime jurídico autónomo para a recolha de prova digital, de modo a acautelar todas as suas especificidades. Ao contrário do que sucede com a recolha de prova física, no caso da prova digital, torna-se necessária a existência de peritos em Ciência Forense Digital, que possuam os devidos conhecimentos para proceder a uma recolha efetiva e integral da prova existente no ambiente digital.

[219] KERR, Orin, "Digital Evidence and The New Criminal Procedure", In: *Columbia Law Review*, Vol. 105:279, pp. 281-289, disponível em https://bityli.com/ZSIFI, último acesso em 16-08-2021.

O termo Ciência Forense Digital surgiu no seguimento do termo Ciência Forense Computacional, sendo que esta se trata do "*(...) método científico subjacente às atividades de recolha, exame, análise e apresentação da prova (...)*"[220]. A origem do termo Ciência Forense Computacional remonta a 1984, com o lançamento do *Magnetic Media Program*, pelo *Federal Bureau of Investigation*, através do qual se pretendia encontrar criminosos ligados à pornografia infantil, e levou à criação da *Computer Analysis and Response Team*, uma equipa que procede a buscas e apreensões de provas digitais, bem como exames forenses e suporte técnico para investigações criminais levadas a cabo pelo *Federal Bureau of Investigation*[221]. Com a contínua evolução tecnológica, o termo Ciência Forense Computacional acabou por se revelar insuficiente para abranger uma realidade um pouco mais complexa do que aquela que esteve na sua origem e que se focava maioritariamente nos computadores. Foi nesta senda que apareceu, então, a Ciência Forense Digital[222].

Para Benjamim Silva Rodrigues, a Ciência Forense Digital "*(...) pretende orientar a investigação criminal, em matéria de criminalidade informático-digital, para a preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação deste específico tipo de prova (prova digital).*"[223]. Já Eoghan Casey entende que esta se traduz num termo abrangente que cobre todas as práticas gerais de análise de todas as formas de prova digital, podendo, no entanto, existir diversas especializações, como é o caso de *Computer Forensics*, que se dedica à preservação e análise de computadores; *Network Forensics*, relativa à preservação e análise de tráfego e acesso a redes; *Mobile Device Forensics*, que se ocupa da preservação e análise de telemóveis, *smartphones* e sistemas de GPS; e, por fim, *Malware Forensics*, especializada em preservação e análise de código malicioso[224].

É no âmbito da Ciência Forense Digital que surgem, tendo em conta as especificidades da prova digital, vários modelos de linhas condutoras e procedimentos gerais para a obtenção e recolha deste tipo de prova, numa tentativa de gerar um *standard* no que respeita às diferentes fases a adotar para aceder, estabilizar e conservar a prova digital o melhor possível para que possa ter o correspondente valor probatório em sede de audiência de discussão e julgamento. Não obstante, e por mais contraditório que pareça, não existe, entre os diversos autores, um consenso

---

[220] RAMALHO, David Silva, Métodos Ocultos de Investigação Criminal em Ambiente Digital, Reimpressão, Almedina, 2019, p. 109;
[221] Vide informação disponível em https://bityli.com/gmeSE, último acesso em 16-08-2021;
[222] RAMALHO, David Silva, Métodos Ocultos de Investigação Criminal em Ambiente Digital, Reimpressão, Almedina, 2019, pp. 109-111;
[223] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade Informática*, 1ª edição, Rei dos Livros, 2011, p. 31;
[224] CASEY, Eoghan, *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, 3ª edição, Elsevier Inc. All, 2011, disponível em https://bityli.com/r8m8h, último acesso em 12-08-2021, p. 38;

relativamente a qual o melhor modelo a adotar, pelo que iremos de seguida, e de forma não exaustiva, evidenciar alguns dos modelos existentes[225].

O modelo Carrier/Spafford, denominado *Integrated Digital Investigation Process*, foi desenvolvido por Brian Carrier e Eugene Spafford, em 2003, e distingue-se dos restantes por relacionar o processo da investigação em ambiente digital com o da investigação em ambiente físico, olhando para o próprio computador ou dispositivo digital como o lugar do crime. O processo é integrado por 17 fases que podem ser organizadas em 5 grupos distintos: preparação (*readiness hases*), revelação do acidente (*deployment phases*), investigação do local físico do crime (*physical crime scene investigation phases*), investigação do local digital do crime (*digital crime scene investigation phases*), e, por último, apresentação (*presentation phase*)[226]. Posteriormente, em 2005, os autores vieram reduzir significativamente o modelo apresentado para apenas 4 fases – pré-processamento dos dados do local do crime (*crime scene data preprocessing phase*), identificação do objeto da investigação (*target definition phase*), processamento dos dados do local do crime (*crime scene data processing phase*), e comparação de dados (*data comparison phase*)[227].

O modelo Casey/Palmer, também denominado de *Staircase Model*, foi criado por Eoghan Casey e Gary Palmer, em 2001, e trata-se de um modelo genérico em que todos os diferentes atores (advogados, investigadores e examinadores forenses) trabalham em conjunto para apresentar, em sede de audiência de discussão e julgamento, uma história convincente. Como etapas deste modelo temos: conhecimento do crime ou acusação (*incident alerts or accusation*), definição da prioridade do caso (*assessment of worth*), protocolos do lugar do crime (*incident/crime scene protocols*), identificação e apreensão (*identification or seizure*), preservação (*preservation*), recuperação (*recovery*), relacionar dados entre si (*harvesting*), redução (*reduction*), organização e busca (*organization and search*), análise (*analysis*), relatório (*reporting*) e persuasão e testemunho (*persuasion and testimony*). Os autores alertam para o facto de as diferentes etapas ocorrerem, por vezes, em simultâneo, e poder ser necessário que certas etapas tenham lugar mais do que uma vez à medida que a investigação vai avançando e que vão surgindo novas informações[228].

---

[225] HOLT, Thomas J., BOSSLER, Adam M., e SEIGFRIED-SPELLAR, Kathryn C., *Cybercrime and Digital Forensics – An Introduction*, Routledge, 2015, p. 330;

[226] CARRIER, Brian D., SPAFFORD, Eugene H., *An Event-Based Digital Forensic Investigation Framework*, From the proceedings of The Digital Forensic Research Conference, DFRWS, Baltimore, 2004, pp. 4-6, disponível em https://bityli.com/05APo, último acesso em 17-08-2021;

[227] CARRIER, Brian D., SPAFFORD, Eugene H., *Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence*, From the proceedings of The Digital Forensic Research Conference, DFRWS, New Orleans, 2005, pp. 1-3, disponível em https://bityli.com/mZZqF, último acesso em 17-08-2021;

[228] CASEY, Eoghan, *Digital Evidence and Computer Crime – Forensic Science*, Computers and the *Internet*, 3ª edição, Elsevier Inc. All, 2011, disponível em https://bityli.com/r8m8h, último acesso em 18-08-2021, pp. 192-193;

O modelo apresentado por Séamus Ó Ciardhuáin, em 2004, denominado de *Evidence Flow Model*, vai para além das etapas necessárias para recolher, preservar e examinar a prova digital, porquanto integra igualmente questões não técnicas de uma investigação criminal em ambiente digital, como sejam autorizações ou notificações. Com este modelo, o autor pretendeu descrever totalmente o fluxo de informação numa investigação criminal em ambiente digital, desde o momento em que os investigadores obtêm a notícia do crime até ao momento da conclusão da investigação. Apresenta como etapas as seguintes: necessidade de investigação (*awareness*), autorização (*authorisation*), planificação (*planning*), notificação (*notification*), procurar e identificar provas (*search for and identify evidence*), recolher provas (*collection of evidence*), transporte da prova (*transport of evidence*), armazenamento da prova *(storage of evidence*), exame da prova (*examination of evidence*), hipótese (*hypothesis*), apresentação da hipótese (*presentation of hypothesis*), prova da hipótese (*proof/defence of hypothesis*) e divulgação da informação (*dissemination of information*)[229].

Na doutrina portuguesa, Benjamim Silva Rodrigues apresentou, em 2008, um modelo, denominado Modelo Forense Dinâmico-Reversivo, que, de acordo com o autor, deve possuir imprescindivelmente as seguintes fases: fase de obtenção da respetiva autorização judicial e de preparação estratégica de abordagem à prova eletrónico-digital; fase de identificação do tipo de prova eletrónico-digital presente no contexto eletrónico ou digital a ser abordado; fase de documentação, recolha e preservação da prova eletrónico-digital; fase de estabilização, filtragem, redução, exame e análise da prova eletrónico-digital identificada em cada contexto eletrónico ou digital; fase de classificação da prova eletrónico-digital; fase de reconstrução dinâmica da prova eletrónico-digital com recurso ao método dinâmico-reversivo; fase de relato e apresentação dos resultados e características da prova eletrónico-digital obtida; e, por último, fase de devolução ou restituição da prova eletrónico-digital dispensável ou desnecessária. Para o autor, trata-se de um modelo dinâmico-reversivo "*(...) no sentido de acentuar o dinamismo, interdependência e correlação existentes entre cada uma das fases e, acima de tudo, o caráter reversivo de tal método, no sentido de que, em muitos casos de obtenção da prova eletrónico-digital, se torna necessário fazer o caminho inverso àquele que levou ao surgimento de um dado tipo de prova eletrónico-digital.*"[230].

---

[229] Ó CIARDHUÁIN, Séamus, "An Extended Model of Cybercrime Investigations", *In: International Journal of Digital Evidence*, Summer 2004, Volume 3, Issue 1, pp. 4-8, disponível em https://bityli.com/jlUxB, último acesso em 18-08-2021;

[230] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade Informática*, 1ª edição, Rei dos Livros, 2011, pp. 491-492;

A constante evolução dos referidos modelos e outros que integram a Ciência Forense Digital e das tecnologias, acompanhada da crescente intromissão do poder estatal nas comunicações eletrónicas dos cidadãos, têm vindo a incentivar, de igual modo, o crescimento de métodos utilizados com o intuito de impedir a deteção de determinadas atividades em ambiente digital e de frustrar a recolha de prova da mesma[231]. Conforme já *supra* mencionado, as novas tecnologias vieram abrir todo um novo leque de utilidades inerentes aos computadores que vieram revolucionar o modo como hoje comunicamos e a rapidez com que agora é possível transmitir informação. Contudo, estas tecnologias também podem ser utilizadas como uma arma e os criminosos, que igualmente se adaptaram às mesmas e transferiram os seus crimes para o ambiente digital, adotaram vários métodos para encobrir os seus passos e esconder a prática de factos ilícitos neste tipo de ambiente. Assim, é possível dizer que estes métodos utilizados podem apresentar uma dupla natureza, na medida em que tanto podem apresentar uma natureza legítima quando utilizados para proteção dos utilizadores ou para a segurança de determinados dados informáticos, como podem ser utilizados para dissimular indícios da prática de crime e obstar a recolha da respetiva prova[232].

É nesta senda que surge o termo medidas anti-forenses ou *antiforensics* que, apesar de não existir entre os vários autores um consenso quanto à sua definição, se pode dizer que são, nas palavras de Ryan Harris, "*(...) methods used to prevent (or act against) the application of scienceto those criminal and civil laws that are enforced by police agencies in a criminal justice system.*". Para o autor, as medidas anti-forenses traduzem-se em ferramentas que tentam comprometer a disponibilidade ou utilidade das provas no processo de investigação forense, na medida em que impedem que existam provas, escondem provas existentes, manipulam provas para garantir que as mesmas não são alcançáveis pelo investigador, fazem desaparecer provas e destroem a integridade das mesmas[233]. Já Simson Garfinkel entende que as medidas anti-forenses se apresentam como "*(...) a growing collection of tools and techniques that frustrate forensic tools, investigations and investigators.*", identificando como objetivos das mesmas os seguintes: evitar a deteção de algum tipo de evento que tenha ocorrido; perturbar a recolha de informação; aumentar o tempo que um investigador dedica a um determinado caso; lançar dúvidas acerca de um relatório ou testemunho forense; forçar a ferramenta forense utilizada no âmbito da investigação criminal para a recolha de prova a revelar a sua presença; e utilizar a ferramenta forense para atacar a

[231] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, pp. 150-151;
[232] *Idem*, p. 151;
[233] HARRIS, Ryan, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", *In: Digital Investigation*, 3S, 2006, pp. 44-45, disponível em https://bityli.com/XEv6M, último acesso em 18-08-2021;

própria entidade que à mesma recorreu[234]. Apesar de a temática das medidas anti-forenses ser relativamente recente, a verdade é que as mesmas já têm grande presença online, sendo tal ilustrado pela existência de *websites* dedicados à difusão destas medidas, mormente à utilização menos legítima das mesmas, como é o exemplo do *anti-forensics.com*, que, de acordo com o mesmo, representa uma comunidade dedicada a pesquisar e partilhar ferramentas que podem ser utilizadas para frustrar investigações criminais em ambiente digital.

Igualmente controversa é a divisão, operada pelos vários autores, relativamente aos tipos de medidas anti-forenses existentes. Ainda assim, a grande maioria parece categorizar estas medidas em quatro grandes grupos, a saber: medidas anti-forenses de destruição de provas, medidas anti-forenses de ocultação de provas, medidas anti-forenses de eliminação da origem/fonte das provas e medidas anti-forenses de falsificação de provas.

As medidas anti-forenses de destruição de provas fazem desaparecer total ou parcialmente as provas, tornando-as inutilizáveis no âmbito de procedimento de investigação criminal e posterior processo penal. Não se trata aqui de tornar as provas inacessíveis, mas sim de as fazer, efetivamente desaparecer. Sucede que, este procedimento de destruição de provas pode provocar a existência de novas provas, isto é, o simples facto de substituir um determinado ficheiro pode fazer com que este desapareça, mas o programa informático utilizado para proceder a tal operação pode criar provas adicionais.

Por seu turno, as medidas anti-forenses de ocultação de provas traduzem-se no "*(...) act of removing evidence from view so that it is less likely to be incorporated into the forensic process.*"[235]. Aqui, não existe uma destruição ou manipulação da prova, apenas se faz com que a prova seja menos visível para quem esteja à procura dela, mormente o investigador. Os ficheiros probatórios podem ser colocados em locais não muito comuns, onde os investigadores não costumam procurar, ou pode ser dado aos mesmos um nome distinto, com o intuito de enganar o investigador que, à partida, entenderá que um ficheiro com aquele nome não tem relevância para a investigação. Cumpre evidenciar que esta medida anti-forense pode ser, ela própria, contraproducente, na medida em que, por vezes, não é necessário encontrar as provas porquanto o *software* de ocultação utilizado é ele próprio prova.

---

[234] GARFINKEL, Simon, "Anti-Forensics: Techniques, Detection and Countermeasures", *In*: *The 2nd International Conference on i-Warfare and Security (ICIW)*, Naval Postgraduate School, Dudley Knox Library, 2007, p. 77, disponível em https://bityli.com/ahBlz, último acesso em 18-08-2021;

[235] HARRIS, Ryan, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", In: *Digital Investigation*, 3S, 2006, pp. 46, disponível em https://bityli.com/XEv6M, último acesso em 18-08-2021;

As medidas anti-forenses de eliminação da origem/fonte da prova dizem respeito às situações em que se neutraliza a própria origem da prova – não há, aqui, necessidade de destruir a prova porque ela nunca foi criada à partida. Foram tomadas, desde logo, precauções para evitar a produção e existência de prova, para que, mais tarde, não exista qualquer tipo de preocupação com investigações criminais que possam ocorrer.

Por último, as medidas anti-forenses de falsificação de provas reportam-se ao "*(...) act of creating a ''faked'' version of the evidence which is designed to appear to be something else*.". Pode consistir em criar uma prova que, em *ultima ratio*, vai funcionar como um ataque contra o procedimento de investigação criminal ou em editar, de forma seletiva, as provas já existentes para corromper a validade das mesmas. Assim, as provas podem estar em *plain sight*, acessível a qualquer um, mas, ainda assim, serem totalmente inválidas. Este tipo de medidas anti-forenses destaca-se pelo facto de ser, frequentemente, combinado com outro tipo de medidas. No ambiente digital, é frequente a prática de crimes com recurso à utilização de contas pessoais de outras pessoas, fazendo com que a investigação criminal considere o criminoso uma outra pessoa que não a que praticou efetivamente o facto ilícito[236].

3.3. Requisitos de admissibilidade e direitos fundamentais restringidos por via do recurso às ações encobertas em ambiente digital

Conforme já *supra* analisado, as ações encobertas encontram-se legalmente previstas na Lei n.º 101/2001, de 25 de Agosto, denominada de Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal. Ora, apesar de o referido regime jurídico não mencionar especificamente o meio para o qual se prevê a realização de ações encobertas, a doutrina tem vindo a entender que o mesmo se refere às ações encobertas realizadas em ambiente físico, por oposição às previstas na Lei do Cibercrime. Com o aparecimento da Lei do Cibercrime, a doutrina começou a proceder a uma distinção entre as ações encobertas realizadas em ambiente físico e as ações encobertas realizadas em ambiente digital, tudo devido à previsão legal aposta no artigo 19.º da Lei do Cibercrime[237].

[236] HARRIS, Ryan, "Arriving at an anti-forensics consensus: Examining how todefine and control the anti-forensics problem", *In*: *Digital Investigation*, 3S, 2006, pp. 45-46, disponível em https://bityli.com/XEv6M, último acesso em 19-08-2021;

[237] Neste sentido, vide RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, pp. 303-304, e NUNES, Duarte Rodrigues, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, Gestlegal, 2018, p. 196;

No que se refere às ações encobertas em ambiente digital, dispõe o n.º 1 do artigo 19.º da Lei do Cibercrime[238], sob a epígrafe *Ações Encobertas* e consagrando um catálogo de crimes distinto do previsto no artigo 2.º do Regime Jurídico das Ações Encobertas, que poderão ser realizadas ações encobertas em ambiente digital relativamente aos crimes de falsidade informática; dano relativo a programas ou outros dados informáticos; sabotagem informática; acesso ilegítimo; reprodução ilegítima de programa protegido; crimes punidos com uma pena de prisão superior a 5 anos que sejam cometidos por meio de um sistema informático; os crimes dolosos, independentemente da pena aplicável, contra a liberdade e autodeterminação sexual, previstos nos artigos 166.º n.º1, 167.º, 170.º, 171.º n.º 2, 173.º, 174.º e 176.º n.º 1, 4 e 6 do Código Penal; crimes em que os ofendidos sejam menores ou incapazes; crime de burla qualificada, prevista no artigo 218.º n.º 1 do Código Penal; crimes de discriminação racial, religiosa e sexual; crimes previstos nos artigos 195.º a 199.º do Código dos Direitos de Autor e Direitos Conexos; e crimes relativos a infrações económico-financeiras.

Da comparação entre o conteúdo do n.º 1 do artigo 19.º da Lei do Cibercrime e do artigo 2.º do Regime Jurídico das Ações Encobertas, é possível observar que o primeiro se revela muito mais amplo e diverso do que o segundo. Com efeito, tão amplo que Paulo Pinto de Albuquerque entende ser o mesmo inconstitucional. Como refere o autor, o "*(...) âmbito muito amplo no tocante aos crimes 'previstos na presente lei', incluindo até um crime de acesso ilegítimo, deve ser objeto de uma restrição teleológica, em função precisamente da falta de gravidade intrínseca do crime; mas mais radicalmente, considerando que a norma é inconstitucional por o 'leque muito amplo de crimes', que inclui pequena criminalidade, violar o princípio da proporcionalidade (...)*"[239]. Parece-nos, efetivamente, ser forçoso concordar com o autor, porquanto existe no catálogo de crimes previsto no n.º 1 do artigo 19.º da Lei do Cibercrime, crimes de uma gravidade menor que poderiam ser, com elevada probabilidade e sucesso, investigados com recurso a meios de obtenção de prova menos gravosos que as ações encobertas.

Não obstante as ações encobertas em ambiente digital se distingam doutrinariamente das ações encobertas em ambiente físico e possuam uma consagração expressa no preceito legal

---

[238] Vide artigo 19.º n.º 1 da Lei do Cibercrime:
"*1 - É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:*
a) Os previstos na presente lei;
b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.";

[239] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição reimpressão, Lisboa, Universidade Católica Editora, 2018, pp. 681-682;

vindo de referir, a verdade é que as mesmas se encontram, ainda assim, sujeitas às normas previstas no Regime Jurídico das Ações Encobertas, só podendo, portanto, existir um recurso a estas quando seja dado cumprimento aos princípios da adequação e proporcionalidade. Conforme já *supra* mencionado em 2.3, na senda do princípio da adequação, as ações encobertas devem ser adequadas às finalidades que com a mesma se pretendam atingir, isto é, o recurso às mesmas deverá ocorrer quando tal for imprescindível para a descoberta da verdade material. Por seu turno, na égide do princípio da proporcionalidade, torna-se necessário fazer um juízo de ponderação – saber se a investigação do crime em apreço justifica o recurso às ações encobertas, ainda que se encontre previsto no catálogo de crimes que permite o recurso a este meio de obtenção de prova; e se não existe nenhum outro meio de obtenção de prova menos gravoso e que se revele igualmente apto, adequado e suficiente.

Nesta senda, Duarte Rodrigues Nunes entende que, uma vez que as ações encobertas são mais lesivas do que a interceção nas comunicações eletrónicas, prevista no artigo 18.º da Lei do Cibercrime, e tendo em conta que o n.º 2 deste preceito legal[240] exige a existência de razões suficientes para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, então também só é legítimo recorrer às ações encobertas em ambiente digital nestes casos em que tal se afigure como indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter[241].

Relativamente à cumulação das ações encobertas em ambiente digital com a utilização de meios técnicos, dispõe o n.º 2 do artigo 19.º da Lei do Cibercrime que "*Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações*.". Situação diferente é a que se equaciona com a cumulação das ações encobertas em ambiente digital com outros meios de obtenção de prova, caso em que a doutrina tem vindo a entender que não existe qualquer impedimento legal para o efeito, desde que, contudo, não ocorra uma violação do princípio da proporcionalidade, na sua vertente de proibição do excesso, e que não leve a situações de uma total vigilância ao indivíduo alvo dos referidos meios de obtenção de prova[242]. Esta proibição de vigilância ficou patente no Acórdão n.º 442/2007, do Tribunal Constitucional, onde o mesmo declarou ser inconstitucional a

---

[240] Vide artigo 18.º n.º 2 da Lei do Cibercrime:
"*2 - A interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.*";

[241] NUNES, Duarte Rodrigues, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, Gestlegal, 2018, pp. 207-208;

[242] *Idem*, pp. 209-210;

possibilidade de a Autoridade Tributária poder aceder às contas bancárias dos contribuintes, sempre que estes impugnassem judicialmente ou reclamassem de um determinado ato tributário[243].

Da análise *supra* realizada à temática das ações encobertas em ambiente físico e do seu regime jurídico, resultou que as mesmas, enquanto método oculto de investigação criminal, neutralizam e restringem alguns dos direitos fundamentais dos cidadãos alvo deste meio de obtenção de prova. Ora, as ações encobertas em ambiente digital não fogem a esta realidade e, também elas, implicam uma ingerência nos direitos fundamentais dos indivíduos, nomeadamente no direito à intimidade ou reserva da vida privada, à autodeterminação informacional ou informativa, à confidencialidade e integridade dos sistemas informacionais e à inviolabilidade do domicílio informático.

O direito à intimidade ou reserva da vida privada encontra-se previsto nos artigos 26.º n.º 2, 32.º n.º 8 e 34.º n.º 4 da Constituição da República Portuguesa e 126.º do Código de Processo Penal e "*(...) tem por fim salvaguardar a intimidade da vida privada e familiar de cada cidadão impedindo a sua devassa, mesmo pelas entidades públicas*."[244]. Gomes Canotilho e Vital Moreira defendem tratar-se de um direito que se analisa em dois direitos menores – o direito a impedir que estranhos obtenham acesso a informações sobre a vida privada e familiar e o direito a que ninguém proceda à divulgação de informações que detenha sobre a vida privada de outrem[245]. Como muitos outros direitos fundamentais, o direito à intimidade/reserva da vida privada pode ser restringido, no caso de existirem valores ou interesses que a este se sobreponham e justifiquem uma tal restrição. Tal sucede com o recurso às ações encobertas em ambiente digital, na medida em que os indivíduos alvo das mesmas partilham determinadas informações pessoais e privadas com alguém em quem acreditam poder confiar, quando, na verdade, se trata de um agente encoberto que tem como objetivo a recolha de prova no âmbito de um procedimento criminal ou com o intuito de, posteriormente, vir a instaurar um. No seio de uma ação encoberta em ambiente digital, o agente encoberto convive diariamente e partilha da intimidade do suspeito alvo da mesma, passando a ter acesso a informações privilegiada sobre a sua pessoa, informações estas às quais nunca teria tido acesso se não tivesse ganho a confiança do suspeito, ocorrendo, deste modo, uma restrição do direito à intimidade/reserva da vida privada.

---

[243] Vide Acórdão n.º 442/2007 do Tribunal Constitucional, de 14 de Agosto, disponível em https://bityli.com/Kiu9n, último acesso em 21-08-2021;
[244] CONCEIÇÃO, Ana Raquel, *Escutas Telefónicas – Regime Processual Penal*, Lisboa, Quid Iuris, 2009, pp. 71-72;
[245] CANOTILHO, J. Gomes, e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume I, 4ª edição, Coimbra Editora, 2007, pp. 467-468.

Um outro direito que é restringido por via do recurso às ações encobertas em ambiente digital e intimamente ligado ao direito à intimidade/reserva da vida privada é o direito à autodeterminação informacional ou informativa. Este direito começou a ser abordado pelo Tribunal Constitucional Federal da Alemanha, o *Bundesverfassungsgericht*, em 1983, no âmbito de um processo relativo a informações pessoais divulgadas durante os Censos, e diz respeito ao "*(...) direito de dispor da informação própria, ou seja, de permitir ou não a sua divulgação e até que ponto, estando subjacente o poder de eliminar informação pessoal de registos alheios (naturalmente dentro dos limites da lei)*."[246]. Ao dar a cada pessoa o direito de controlar a informação que se encontra disponível, o direito à autodeterminação informacional ou informativa vincula entidades públicas e privadas, impedindo que a própria pessoa a quem pertencem determinados dados se transforme num objeto de informações – não se trata apenas de um direito de carácter defensivo em relação ao tratamento de dados pessoais, mas é antes um direito de conformar esse mesmo tratamento, dando ao indivíduo o poder de controlar a partilha e utilização dos seus dados pessoais[247]. Em Portugal, o direito em apreço encontra-se previsto no n.º 2 do artigo 35.º da Constituição da República Portuguesa e amplamente consagrado na jurisprudência dos tribunais superiores, mormente nos acórdãos do Tribunal Constitucional n.º 442/2007[248] e 403/2015[249]. As ações encobertas em ambiente digital implicam uma restrição ao âmbito do direito à autodeterminação informacional ou informativa, uma vez que, enquanto meio de obtenção de prova predominantemente digital, implicam a recolha de dados pessoais dos indivíduos alvo das mesmas, não podendo estes controlar a realização da ação encoberta, dado não saberem sequer que os seus dados se encontram a ser recolhidos e tratados.

Por seu turno, o direito à confidencialidade e integridade dos sistemas informáticos foi, pela primeira vez, reconhecido em 2008, pelo Tribunal Constitucional Federal da Alemanha, quando o mesmo foi chamado a apreciar a constitucionalidade de várias normas da Lei da

---

[246] PINHEIRO, Alexandre Sousa, *Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Associação Académica da Faculdade de Direito de Lisboa, 2015, pp. 474-475;

[247] CANOTILHO, J. Gomes, e MOREIRA, Vital, Constituição da República Portuguesa Anotada, Volume I, 4ª edição, Coimbra Editora, 2007, p. 551; e CASTRO, Catarina Sarmento e, "40 anos de "Utilização da Informática" - o artigo 35.º da Constituição da República Portuguesa", *In*: *E-Pública – Revista Eletrónica de Direito Público*, Vol. 3, n.º 3, Dezembro de 2016, pp. 50-51, disponível em https://bityli.com/06SxB, último acesso em 24-08-2021;

[248] Vide Acórdão n.º 442/2007 do Tribunal Constitucional, de 14 de Agosto, disponível em https://bityli.com/Kiu9n, último acesso em 24-08-2021, onde se pode ler que "*Por autodeterminação informativa poderá entender-se o direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada. Compete a cada um decidir livremente quando e de que modo pode ser captada e posta a circular informação respeitante à sua vida privada e familiar.*";

[249] Vide Acórdão n.º 403/2015 do Tribunal Constitucional, de 27 de Agosto, disponível em https://bityli.com/jHMea, último acesso em 24-08-2021, onde se pode ler que "*Quanto ao âmbito objetivo do direito à reserva sobre a intimidade da vida privada, o Tribunal tem dito (...) que tal direito inclui, como diferentes manifestações, o direito à solidão, o direito ao anonimato e o direito à autodeterminação informativa. Depois, com a esfera íntima e a esfera privada da pessoa humana, seja enquanto pretensão de isolamento, tranquilidade e exclusão do acesso dos outros a si próprio (direito à solidão), seja, enquanto impedimento à ingerência dos outros (direito ao anonimato), seja ainda, mais modernamente, e perante a insuficiência protetora das referidas dimensões, enquanto controlo das informações que lhe dizem respeito e de subtração ao conhecimento dos outros os factos reveladores do modo de ser do sujeito na condução da sua vida privada (autodeterminação informacional).*";

Proteção da Constituição da Renânia do Norte-Vestefália, normas estas que permitiam que as autoridades policiais realizassem buscas e acedessem remotamente aos computadores de indivíduos suspeitos da prática de factos ilícitos, autorizando, ainda, a monotorização de todas as atividades dos suspeitos na *internet* [250]. Surgindo com o propósito de proteger a confiança dos indivíduos na funcionalidade dos sistemas informáticos utilizados para a comunicação[251], com este direito "*(...) visa-se proteger-se, por um lado, o interesse do utilizador em garantir que os dados gerados, tratados e armazenados pelos sistemas informáticos abrangidos permaneçam confidenciais e, por outro, que a integridade do sistema não seja comprometida através de acessos não autorizados por parte de terceiros.*"[252]. Estamos, assim, perante um direito que abrange os sistemas informáticos onde se possam encontrar dados pessoais dos seus utilizadores, dados estes capazes de permitir o conhecimento significativo da vida dos mesmos e até da sua personalidade. Apesar de a confidencialidade e integridade dos sistemas informáticos ser já tutelada nos termos dos artigos 5.º e 6.º da Lei do Cibercrime, podemos igualmente afirmar que o direito em apreço decorre de vários princípios consagrados, como o princípio do Estado de Direito democrático, assim como do direito ao livre desenvolvimento da personalidade, à utilização da informática, ao sigilo da correspondência, entre outros[253]. No que respeita à relação do direito à confidencialidade e integridade dos sistemas informáticos com as ações encobertas em ambiente digital, é clara a conclusão que estas restringem largamente o referido direito, na medida que a confiança que os utilizadores depositam na confidencialidade dos sistemas informáticos é totalmente defraudada com as atividades de recolha de prova digital e a infiltração de terceiros que, para esse intuito, ocultam a sua identidade.

Finalmente, o direito à inviolabilidade do domicílio informático, ainda gerador de alguma controvérsia entre os autores, diz respeito à proteção deste domicílio, de algum modo correspondente à introdução em casa alheia. De acordo com Lourenço Marins, Garcia Marques e Pedro Simões Dias, a tutela do domicílio informático reporta-se à "*(...) privacidade do mesmo domicílio e ainda à liberdade informática de cada um operar no interior desse domicílio e de excluir do mesmo os terceiros mal vindos.*"[254]. Este bem jurídico encontra-se tutelado pela incriminação

[250] MENKE, Fabiano, "A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito Alemão", *In*: *RJLB*, Ano 5, n.º 1, 2019, pp. 793-794, disponível em https://bityli.com/pyW2s, último acesso em 24-08-2021;

[251] HOFFMANN-RIEM, Wolfgang, RIBEIRO, Pedro Henrique, "A Proteção de Direitos Fundamentais de Confidencialidade e da Integridade de Sistemas Próprios de Tecnologia da Informação", *In*: *Revista de Direito Civil Contemporâneo*, Vol. 23, Ano 7, pp. 347-348, disponível https://bityli.com/sy7T3, último acesso em 24-08-2021;

[252] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 247;

[253] *Idem*, pp. 247-249.

[254] MARTINS, A. G. Lourenço, MARQUES, J. A. Garcia, e DIAS, Pedro Simões, *Cyberlaw em Portugal – O Direito das Tecnologias da Informação e da Comunicação*, Centro Atlântico, 2004, pp. 443-444;

do acesso ilegítimo, prevista no artigo 6.º da Lei do Cibercrime, ao prever que quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. O direito em apreço, já alvo de estudo por parte da jurisprudência dos tribunais superiores[255], vê o seu conteúdo gravemente restringido com o recurso às ações encobertas em ambiente digital, porquanto as mesmas implicam, conforme já *supra* mencionado, uma infiltração em sistemas e redes informáticas para uma posterior recolha de prova digital, infiltração esta que não é autorizada, nem sequer conhecida, pelo utilizador que confia e acredita na segurança do seu domicílio informático.

3.4. Utilização de *malware* no seio das ações encobertas em ambiente digital

A realização de ações encobertas em ambiente digital e a consequente recolha da prova digital trazem consigo inúmeras especificidades, algumas já *supra* abordadas, outras a que nos iremos dedicar *infra*, no capítulo seguinte do presente estudo. Uma destas especificidades diz respeito à (im)possibilidade de utilização de *malware* no âmbito das mesmas.

De acordo com a definição avançada por David Ramalho, o conceito de *malware* "*(...) inclui todo o tipo de programas instalados por terceiros de forma sub-reptícia num sistema informático que podem ser utilizados para, de algum modo, comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao sistema informático afeado, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos.*"[256]. Já Joshua B. Hill e Nancy E. Marion identificam o *malware* como um "*(...) general term for a siftware that affect how a computer functions.*"[257]. Tratando-se de um programa informático malicioso, o *malware* explora todas as vulnerabilidades e defeitos que encontre num determinado sistema informático. Uma vez encontrada a vulnerabilidade do sistema, a pessoa que pretende instalar o *malware* cria um código malicioso que consegue tirar vantagens dessa mesma

[255] Vide, neste sentido, Acórdão do Tribunal da Relação do Porto, datado de 08-01-2014, relativo ao processo n.º 1170/09.8JAPRT.P2, disponível em https://bityli.com/PpIYv, último acesso em 25-08-2021, onde se pode ler que: "*O crime de acesso ilegítimo veio, no essencial cobrir a área do que se vem denominando de "hacking informático". Em geral, tratava-se de cobrir as condutas que se traduziam na mera entrada ou acesso a sistemas informáticos por «mero prazer» ou «gozo» em superar as medidas ou barreiras de segurança, isto é, sem qualquer (outra) intenção ou finalidade alguma de manipular, defraudar, sabotar ou espionar, situação que veio a suscitar dúvidas sobre a necessidade ou não de criminalizar tais condutas. Com a norma tutela-se a «integridade do sistema informático lesado», a partir de uma ideia nova de «inviolabilidade do domicílio informático»*".

[256] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 319;

[257] HILL, Joshua B., e MARION, Nancy E., *Introduction to Cybercrime – Computer Crimes, Laws and Policing in the 21st Century*, PSI Textbook, 2016, p. 7;

vulnerabilidade, permitindo, assim, ao atacante compreender e ganhar acesso ao sistema em apreço[258].

O *malware* pode revestir-se de diferentes formas, cada uma com as suas características próprias que acabam por refletir as intenções e objetivos do criador do mesmo. Tais formas podem ser, entre outras, os cavalos de troia (*trojan horses*), *logic bombs*, *worms*, *spyware* e vírus.

Os cavalos de troia traduzem-se num "*(...) tipo de malware que se apresenta como sendo inofensivo e induz o visado a empreender numa conduta ativa que resultará na sua instalação no sistema informático visado, designadamente fazendo um download de um anexo de uma mensagem de correio eletrónico ou abrindo uma página web infetada com código malicioso*."[259]. Escondido no programa dito inocente, está uma espécie de subprograma que vai executar uma determinada função no sistema informático, função esta totalmente desconhecida do utilizador. Uma função comum executada através dos *trojan horses*, é a criação de *backdoors*, o mesmo é dizer, formas escondidas que determinada pessoa utiliza para aceder remotamente ao sistema informático infetado, sendo, assim, possível ultrapassar quaisquer mecanismos existentes de autenticação ou acesso. Com este acesso, é possível obter informações e dados pessoais do utilizador, instalar *malware* adicional ou monitorizar a atividade do utilizador na *internet*[260]. Tendo em conta que os cavalos de troia não conseguem replicar-se sozinhos, torna-se necessária a existência de uma interação por parte do utilizador para executar o referido código malicioso[261]. Um dos cavalos de troia mais conhecidos apresentava a denominação de *Back Orifice 2000* (BO2K), foi escrito e desenvolvido por um grupo de hackers que se intitulava de *Cult of The Dead Cow*, com o intuito de infetar sistemas da *Microsoft*. Atualmente, o *trojan horse* mais conhecido e perigoso tem o nome de *Zeus* e foi desenhado para atacar sistemas do *Microsoft Windows*, sendo enviado através de e-mail de *phishing*. Uma vez instalado, cria uma *backdoor* para o atacante poder obter os dados pessoais dos utilizadores e as suas *passwords* [262].

Por seu turno, as *logic bombs* apresentam-se como "*(...) uma modalidade de malware não replicativo que se instala num sistema informático e aguarda um incidente ou um evento que funcione como um mecanismo de desencadeamento (um gatilho) para desempenhar uma função*

[258] HOLT, Thomas J., BOSSLER, Adam M., e SEIGFRIED-SPELLAR, Kathryn C., *Cybercrime and Digital Forensics – An Introduction*, Routledge, 2015, pp. 80-82;
[259] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, pp. 319-320;
[260] *Ibidem*;
[261] Quem cria e escreve este tipo de *malware*, utiliza princípios da denominada Engenharia Social, com o intuito de seduzir o utilizar a abrir determinado ficheiro que permitirá o desenvolvimento do cavalo de troia;
[262] HOLT, Thomas J., BOSSLER, Adam M., e SEIGFRIED-SPELLAR, Kathryn C., *Cybercrime and Digital Forensics – An Introduction*, Routledge, 2015, pp. 86-88;

nociva ou ofensiva no sistema informático infetado."[263]. Podendo ser inseridas num código já existente ou num autónomo, este tipo de *malware* caracteriza-se por ser extremamente discreto, principalmente quando considerarmos que pode ser inserido num código que apresente milhares de linhas.

Já o *spyware* traduz-se, nas palavras de Juliana Campos, num "*(...) programa que é instalado no sistema informático com o objetivo de monitorizar ou vigiar a atividade do utilizador e de transmitir a informação ao atacante*.". Podendo ser instalado em determinado sistema informático através da utilização de Cavalos de Troia, de vírus ou até do acesso a *websites* maliciosos, o exemplo mais conhecido deste tipo de *malware* são os denominados *keyloggers*, que permitem à pessoa que o criou gravar tudo o que é premido num teclado de um determinado computador[264].

Um outro tipo de *malware* são os *worms*, que mais não são do que uma "*(...) unique form of malware that can autonomously spread on their own, though they do not necessarily have a payload. Instead, they utilize system memory to spread, self-replicate, and deteriorate system functionality*."[265]. O facto de se multiplicarem rapidamente sem a necessidade de uma qualquer interação humana, torna este tipo de *malware* extremamente perigoso e eficaz. O primeiro *worm* conhecido, denominado de *Morris Worm*, foi criado por Robert Tappan Morris, um estudante da *Cornell University*, e ativado em 02 de Novembro de 1998, tendo como objetivo demonstrar a imensa vulnerabilidade dos computadores a programas de *malware*. O *Morris Worm* multiplicou-se na *internet* mais rapidamente do que o esperado pelo seu criador e este tentou remediar o problema ao libertar uma solução precisamente na *internet*. Contudo, esta já se encontrava tão congestionada pelo *worm* que, quando foi possível a solução atuar, já tinham sido criados imensos danos em computadores protegidos de todo o país. Robert Morris foi acusado e acabou por ser a primeira pessoa a ser condenada por violar o *Computer Fraud and Abuse Act* [266] [267].

Por último, e por certo a forma mais antiga e conhecida de *malware*, o vírus é um "*(...) program than infects a computer by inserting a copy of itself into the computer and harms the computer in some manner, generally without the computer user's awareness*.". Como os vírus necessitam da intervenção do utilizador do sistema informático infetado, este utilizador tem que

---

[263] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 320;
[264] CAMPOS, Juliana Filipa Sousa, *O Malware como Meio de Obtenção de Prova em Processo Penal – A Investigação Oculta em Ambiente Digital*, Almedina, 2021, p. 39;
[265] HOLT, Thomas J., BOSSLER, Adam M., e SEIGFRIED-SPELLAR, Kathryn C., *Cybercrime and Digital Forensics – An Introduction*, Routledge, 2015, pp. 88.
[266] Disponível em https://bityli.com/jzrjW, pp. 4-56, último acesso em 27-08-2021;
[267] SINROD, Eric J., e REILLY, William P., "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", *In*: *Santa Clara High Tech Law Journal*, Vol. 16, Issue 2, Article 1, 2000, pp. 221-222, disponível em https://bityli.com/z7w8u, último acesso em 27-08-2021;

executar o código de alguma forma, como seja abrir um determinado ficheiro ou certo anexo num e-mail. O vírus mais conhecido, denominado de *Melissa Macro Virus*, surgiu em 1999 e propagou-se por todos os países do mundo de uma forma muito rápida. Tratava-se de um vírus escondido num anexo do *Microsoft Word* que parecia ser enviado ao utilizador do sistema informático infetado por uma pessoa conhecida deste, e que, quando aberto, surgia ao utilizador uma lista de *passwords* de *sites* pornográficos Não obstante, sem o conhecimento do utilizador, o programa informático lia os primeiros cinquenta e-mails localizados na aplicação *Microsoft Outlook* e enviava-se, a si próprio, a esses mesmos cinquenta endereços de e-mail. Com tal atuação, o vírus em apreço causou mais de 80 milhões de dólares em danos e espalhou-se tão rapidamente que a *Microsoft* e a *Intel* foram obrigadas a desligar os seus servidores[268].

No que respeita ao modo como estes tipos de *malware* são instalados nos sistemas informáticos dos indivíduos visados, David Ramalho distingue três diferentes métodos, a saber: a infeção via suporte físico removível, a infeção via *web browser* e a infeção via *download* voluntário. A infeção via suporte físico removível representava o método mais utilizado antes do aparecimento da *internet* e é, ainda hoje, utilizado, para infetar sistemas informáticos que não tenham conexão à *internet*. Como vantagem apresenta o facto de permitir ao intruso saber que infetou apenas o sistema informático pretendido e que, bem assim, não existe qualquer tipo de possibilidade de a infeção se multiplicar e espalhar. A infeção via *web browser* ocorre quando existe um *download* automático de *malware* quando o utilizador clica num determinado *link*, ou quando existe um acesso a uma página *web*, que aparenta ser legítima e inocente, mas na verdade é composta por *malware* que deteta vulnerabilidades no sistema informático utilizado para aceder e infeta-o. Por último, a infeção via *download* voluntário acontece nos casos em que o utilizador faz, intencionalmente, *download* de algum ficheiro, de programas executáveis ou até de falsas atualizações de *software* [269].

Para melhor compreender a efetiva utilização de *malware* no âmbito de investigações criminais em ambiente digital, torna-se relevante atentar no que sucede noutros ordenamentos jurídicos distintos do nosso.

Nos últimos anos, temos assistido, nos Estados Unidos da América, a várias revelações da utilização secreta, e bem assim não autorizada, de vários tipos de *software* malicioso por parte dos órgãos de polícia criminal. O primeiro registo de utilização de *malware* neste país surgiu em

[268] *Idem*, pp. 215-219.
[269] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 322-324;

2001 e diz respeito ao denominado *Magic Lantern*, um "*(...) keylogger concebido para poder ser instalado sub-reptícia e remotamente via Internet no sistema informático visado – localizado ou não nos EUA – quando este pertencesse a indivíduos suspeitos de estarem relacionados com atividades criminosas, em particular de natureza terrorista.*"[270]. Este tipo de *malware* podia ser instalado através do envio de e-mails para o suspeito com ficheiros infetados, ou mediante a exploração de vulnerabilidades existentes no sistema operativo instalado no computador alvo. Tratando-se de um *software* malicioso, era frequente a sua deteção por parte de vários programas antivírus, de maneira que, para salvaguardar a eficácia e o objetivo subjacente à utilização do *Magic Lantern*, o governo norte-americano terá alegadamente solicitado às empresas autoras dos mesmos que modificassem os seus programas antivírus para não interferir com o *malware* em apreço[271]. O *Magic Lantern* deu, mais tarde, origem a outro *malware*, denominado de *Computer and Internet Protocol Adress Veriffier* (CIPAV), que apenas chegou ao conhecimento público em 2007, tendo sido divulgado, pela comunicação social, um pedido formulado pelo agente do *Federal Bureau of Investigation* Norman Sanders para a sua utilização, no âmbito de um processo onde se tentava obter a identificação do autor de várias ameaças de bomba[272]. Tendo surgido como necessário no seguimento dos acontecimentos ocorridos a 11 de Setembro de 2001, onde o governo norte-americano não foi capaz de prever e evitar os ataques levados a cabo, o *Magic Lantern* ficou igualmente conhecido pela sua utilização no célebre processo *United States* v. *Scarfo*, onde o tribunal determinou que a autorização obtida para a instalação do *malware* em apreço não violava a Quarta Emenda à Constituição dos Estados Unidos[273] [274].

Já na Alemanha, assistimos em finais de 2008, à aprovação da Lei para a Defesa face aos Perigos do Terrorismo Internacional, que consagrou no ordenamento jurídico alemão a possibilidade de recorrer à utilização de *malware* com o intuito de prevenir crimes de terrorismo, sendo esta utilização sempre a título excecional. Anos mais tarde, em 2018, um grupo de *hackers* denominado *Chaos Computer Club* (CCC), trouxe a público a utilização regular, pelos órgãos de polícia criminal, de um tipo de *malware*, intitulado de *Bundestrojaner*. Este programa malicioso era enviado para o computador do suspeito, aparentando ser uma simples atualização de *software*,

---

[270] *Idem*, p. 325;

[271] WOO, Christopher, SO, Miranda, "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance", *In: Harvard Journal of Law & Technology*, Volume 15, Number 2, Spring 2002, p. 524, disponível em https://bityli.com/JYLHG, último acesso em 10-01-2022;

[272] Pedido disponível para consulta em https://bityli.com/LmMSA, último acesso e 10-01-2022.

[273] De acordo com a qual é dado aos cidadãos "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*", disponível em https://bityli.com/KEqax, último acesso em 10-01-2022;

[274] WOO, Christopher, SO, Miranda, "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance", *In: Harvard Journal of Law & Technology*, Volume 15, Number 2, Spring 2002, p. 533, disponível em https://bityli.com/JYLHG, último acesso em 10-01-2022;

e que, uma vez instalado permitia guardar palavras-passe, obter acesso à *webcam* e ao microfone do computador, entre outros[275]. As informações revelados pelo CCC demonstraram que o *malware* em apreço foi utilizado abusivamente por parte da polícia alemã, em investigações a crimes de roubo, fraude e tráfico de substância psicotrópicas, sendo clara a conclusão que foram excedidos os poderes atribuídos aos órgãos de polícia criminal, pelo Tribunal Federal Constitucional Alemão[276].

A Convenção sobre o Cibercrime, formalizada em 2001, marcou o início de várias iniciativas para legislar no que respeita à utilização de *malware* como meio de obtenção de prova. Em Dezembro de 2008, a Comissão Europeia e a *International Telecommunication Union* (ITU) encetaram esforços para criar o Projeto HIPCAR (Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures), que tinha como objetivo proceder a uma uniformização de toda a legislação existente nos países da comunidade das Caraíbas (CARICOM), em nove distintas áreas relacionas com as tecnologias de informação. O projeto HIPCAR acabou por ser "*(...) o mais detalhado modelo legislativo em matéria de cibercrime e prova digital existente, cujo propósito é servir como guião para os diversos Estados que o queiram implementar.*"[277], prevendo, no seu artigo 27.º, a utilização de *malware* nas investigações criminais, através da expressão *remote forensic software* [278].

No que respeita à previsão legal da utilização de *malware* no âmbito de investigações criminais em ambiente digital em Portugal, cumpre salientar que não existe um regime jurídico que preveja expressamente o recurso a este meio atípico de obtenção de prova. Não obstante, são vários os autores que defendem a aplicação de outros regimes jurídicos, numa tentativa de legitimar a existência deste meio de obtenção de prova no seio do processo penal português.

Paulo Pinto de Albuquerque, identificando a utilização de *malware* com o conceito de *busca online*, define esta última como "*(...) a infiltração eletrónica em sistemas informáticos, por*

---

[275] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 329;
[276] BRENNER, Susan, "Law, Dissonance, and Remote Computer Searches", In: *North Carolina Journal of Law and Technology*, Vol. 14, Issue 1, Article 14, 2012, p. 89, disponível em https://bityli.com/nISKV, último acesso em 10-01-2022.
[277] RAMALHO, DAVID, "O Uso de *Malware* como Meio de Obtenção de Prova em Processo Penal", *In: Revista da Concorrência e Regulação*, Ano IV, N.º 16, 2013, p. 224, disponível em https://bityli.com/MSSCH, último acesso em 10-01-2022;
[278] Cfr. artigo 27.º n.º 1 do Projeto HIPCAR, disponível em https://bityli.com/IHMMH, último acesso em 10-01-2022:
"If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the
following information:
a. suspect of the offence, if possible with name and address; and
b. description of the targeted computer system; and
c. description of the intended measure, extent and duration of the utilization; and
d. reasons for the necessity of the utilization.";

exemplo, através dos chamados cavalos de Troia, de modo a que o investigador possa em tempo real ou deferido conhecer a informação que está a ser introduzida ou que já foi introduzida no sistema, incluindo textos, sons e imagens."[279]. No entendimento do Autor, a busca online está consagrada no artigo 15.º da Lei do Cibercrime, inserindo-se na expressão *pesquisa em sistema informático*, e caso este preceito legal permita que o Ministério Público ou os Órgãos de Polícia Criminal ordenem uma pesquisa a um determinado sistema informático, no qual se incluem dados informáticos privados e íntimos, sem controlo prévio ou posterior por parte de um juiz, estaríamos perante uma inconstitucionalidade. Na hipótese de os dados serem submetidos ao juiz para a competente validação, já não há lugar à referida consequência[280].

Por seu turno, Rita Castanheira Neves defende que a Lei do Cibercrime não consagrou expressamente a possibilidade de se recorrer a buscas online, com o intuito de serem recolhidos dados informáticos sem o conhecimento do visado. Para a autora, o facto de se referir, no artigo 15.º da Lei do Cibercrime, a presença da autoridade judiciária na diligência de pesquisa de dados informáticos e, ainda, as formas como os dados informáticos podem ser apreendidos, nos termos do artigo 16.º n.º 7 do mencionado texto legal, não deixam margem para que se possam realizar buscas sem que o visado tenha conhecimento da respetiva diligência[281].

Já David Silva Ramalho entende que a formulação do n.º 2 do artigo 19.º da Lei do Cibercrime introduz a utilização de *malware* nas investigações criminais como um novo meio oculto de obtenção de prova, meio este que não se confunde nem se inclui em qualquer outro meio de obtenção de prova previsto no Código de Processo Penal. De acordo com a tese defendida pelo autor, "Esta conclusão impõe-se pelo mero facto de o legislador ter sentido necessidade de introduzir uma norma nova para legitimar o recurso a estes meios e dispositivos informáticos. Uma norma que terá surgido em face da insuficiência dos demais meios processuais existentes para a utilização destes 'meios e dispositivos informáticos'"[282].

Ora, salvo o devido respeito pela opinião contrária, não podemos perfilhar do entendimento do autor vindo de referir. A utilização de *malware* como um meio de obtenção de prova traduz-se num meio particularmente gravoso e danoso para os direitos fundamentais dos cidadãos, pelo que o recurso ao mesmo teria necessariamente que ter lugar mediante o respeito

---

[279] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição atualizada, Lisboa, Universidade Católica Editora, 2011, p. 502;
[280] *Ibidem*.
[281] NEVES, Rita Castanheira, *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e Respetivo Regime Jurídico do Correio Eletrónico Enquanto Meio de Obtenção de Prova*, Coimbra Editora, 2011, p. 284;
[282] RAMALHO, DAVID, "O Uso de Malware como Meio de Obtenção de Prova em Processo Penal", In: Revista da Concorrência e Regulação, Ano IV, N.º 16, 2013, p. 230, disponível em https://bityli.com/MSSCH, último acesso em 10-01-2022;

escrupuloso de um regime jurídico expressamente previsto para o efeito. A efetiva tutela dos direitos, liberdades e garantias dos indivíduos não se coaduna, no nosso entendimento e no caso em apreço, com uma mera remissão para um outro regime jurídico, nem com a aplicação do extremamente vago n.º 2 do artigo 19.º da Lei do Cibercrime. A utilização de *malware* como meio de obtenção de prova em investigações criminais no ambiente digital não se encontra, de facto, prevista no ordenamento jurídico português. Não obstante, cremos que tal meio pode ser essencial, pelo que deveria o legislador encetar as competentes diligências para a criação de um regime jurídico que acautelasse todas as especificidades do recurso a este meio e, ainda, os direitos dos cidadãos.

No que concerne ao conteúdo concreto deste regime jurídico, adotamos a tese defendida por Juliana Campos, de acordo com a qual devem ser respeitados requisitos formais, materiais e orgânicos, o que implica, entre outros, a reserva de lei[283]; a clareza e precisão do texto normativo; a adoção de expressões concretas, distintas de outras já utilizadas; o estabelecimento de um catálogo de crimes concreto que permita o recurso a este meio de obtenção de prova; a existência de uma fundada suspeita e indícios da prática de crime catalogado; a identificação do alvo, da concreta funcionalidade do *malware* utilizada e do limite temporal para a tal utilização; a exigência de autorização prévia por parte do juiz ou do Ministério Público, com posterior validação por parte do juiz.

[283] Cfr. artigos 18.º n.º 2 e 165.º n.º 1 alínea b) da Constituição da República Portuguesa.

4. NECESSIDADE DE CRIAÇÃO DE REGIME JURÍDICO PARA AS AÇÕES ENCOBERTAS EM AMBIENTE DIGITAL

A criminalidade organizada tem vindo a assumir, cada vez mais, um papel central no dia a dia das investigações criminais realizadas pelos órgãos de polícia criminal. Procurando encontrar uma definição ou conceito base, a denominada Convenção de Palermo refere-se aos grupos criminosos organizados como estruturas organizadas, de três ou mais pessoas, que atuam de forma concertada com o intuito de praticar os vários tipos de ilícitos enunciados na referida Convenção, ilícitos estes que lhes trarão benefícios económicos ou materiais[284]. Por seu turno, o Federal Bureau of Investigation define a criminalidade organizada como "*(...) any group having some manner of a formalized structure and whose primary objective is to obtain Money through ilegal activities. Such groups maintain their position through the use of actual or threatened violence, corrupt public officials, graft or extortion, and generally have a significant impact on the people in their locales, region or the country as a whole*."[285].

Não obstante vários autores avancem com diversas definições, mais ou menos coincidentes, de criminalidade organizada ou grupo criminoso organizado, a verdade é que não existe uma definição pacificamente adotada por todos. Ora, tal não significa que não seja possível encontrar um conjunto de características transversais a todos aqueles que se organizam entre si para a prática de factos ilícitos. Neste sentido, Howard Abadinsky defende que existem oito atributos básicos subjacentes a uma organização criminosa, sendo eles: a inexistência de objetivos políticos, a presença de uma hierarquia; a exclusividade e limitação do número de membros; a constituição de uma subcultura única; a ideia de perpetuidade; a predisposição para recorrer à violência; o objetivo de atingir o monopólio; e, por último, a existências de regras.

De acordo com a tese apresentada pelo autor, o principal objetivo de uma organização criminosa é a obtenção de dinheiro e poder, sendo que não existem quaisquer ambições políticas. Pode, eventualmente, ocorrer um envolvimento político da organização, mas sempre com o intuito de obter proteção e imunidade para a prática de atividades legais, através das quais é atingido o objetivo inicial. Para que o grupo possa funcionar corretamente, é instituída uma hierarquia com, pelo menos, três diferentes níveis ou posições, cada um com autoridade sobre os níveis inferiores. A existência de uma estrita hierarquia encontra-se, de certo modo, relacionada com a exclusividade

[284] Cfr. alínea a) do artigo 2.º da Convenção das Nações Unidas Contra a Criminalidade Organizada Transnacional, disponível em https://bityli.com/h5Nzi, último acesso em 26-01-2022;
[285] ABADINSKY, Howard, *Organized Crime*, 10th Edition, Wadsworth Cengage Learning, 2013, disponível em https://bit.ly/3r4XAnH, último acesso em 26-01-2022, p. 2.

ou limitação do número de membros da organização criminosa. Isto é, para se poderem inserir no grupo e, consequentemente, na hierarquia existente, os potenciais membros devem possuir determinadas qualidades e devem estar dispostos a adotar certos comportamentos, nomeadamente participar em rituais de iniciação. A ideia de exclusividade e limitação das pessoas que podem assumir a qualidade de membros de um grupo criminoso organizado enfatiza a importância atribuída ao facto de alguém se conseguir inserir nesse meio e manter a sua posição. Toda esta cultura é muito própria das organizações criminosas, que se vêem quase como um grupo distinto do resto da sociedade convencional, sendo o mesmo desenhado para persistir no tempo, ou seja, continuar a existir mesmo depois de os atuais membros falecerem. No seio da criminalidade organizada, o recurso à violência é encarado como algo rotineiro, sendo através da mesma que os grandes grupos atingem o monopólio e a tão desejada hegemonia. Para que todos os objetivos possam ser alcançados, os diversos membros têm, necessariamente, que cumprir um conjunto severo de regras, que prevalecem em todas e quaisquer circunstâncias[286].

Estes diferentes atributos, transversais a todos os grupos criminosos organizados, são indicadores do, cada vez maior, grau de sofisticação que os mesmos demonstram para a prática de factos ilícitos. Sofisticação esta que, no entendimento de Duarte Rodrigues Nunes, "*(...) cria especiais dificuldades investigatórias, que, em primeira linha, tornaram obsoletos os meios 'abertos' de investigação criminal, que passaram a ser meios complementares de outros – os 'ocultos' (...)*"[287]. Com efeito, atualmente, o recurso a métodos de investigação criminal ditos abertos, não é, de todo, suficiente para combater a criminalidade organizada que, ao longo dos tempos, foi adotando novas formas de ludibriar os órgãos de polícia criminal e de frustrar as atividades de obtenção e recolha de prova. Tornou-se claro, nas últimas décadas, que, sem lançar mão dos métodos ocultos de investigação criminal, não seria possível combater este tipo de criminalidade – daí que tenha crescido exponencialmente o recurso às ações encobertas, que, em ultima *ratio*, permitem às autoridades competentes infiltrarem-se nas diferentes organizações e, bem assim, contrariar todos os mecanismos utilizados pelos meliantes para se escaparem à atividade investigatória.

Sucede que, tal como já tivemos oportunidade de referir *supra*, as novas tecnologias têm vindo a assumir um papel de destaque no seio da criminalidade organizada, que, cada vez mais, a incorpora nas suas atividades ilícitas, seja mediante a prática de crimes informáticos, seja

[286] ABADINSKY, Howard, Organized Crime, 10th Edition, Wadsworth Cengage Learning, 2013, disponível em https://bit.ly/3r4XAnH, último acesso em 26-01-2022, pp. 3-5;
[287] NUNES, Duarte Rodrigues, "A Incongruência do Património no Confisco 'Alargado' de Vantagens Provenientes da Prática de Crimes", *In*: Centro de Estudos Judiciários (Org.), *Recuperação de Ativos*, 2021, p. 13, disponível em https://bityli.com/CApLT, último acesso em 28-01-2022;

através da utilização de ferramentas informáticas, que surgiram com o aparecimento das novas tecnologias, para facilitar a prática de outro tipo de crimes, que não ocorrem necessariamente no ambiente digital. O fenómeno da globalização veio permitir às organizações criminosas alargar o seu impacto e expandir a um nível global e nunca antes visto. Ainda que não desloquem a prática de crimes para o ambiente digital, podemos agora observar que as atividades ditas tradicionais deste tipo de organizações apresentam um alcance muito superior, quando comparado com uma época em que as ferramentas tecnológicas não existiam. Nesta senda, também os órgãos de polícia criminal se vêem forçados a adotar novas técnicas de investigação e a deslocar determinados métodos de investigação criminal, que tradicionalmente ocorrem num meio físico, para o plano digital, como seja o caso das ações encobertas. Se até ao aparecimento das novas tecnologias se realizavam apenas no ambiente físico, o mesmo já não se pode dizer atualmente, sendo as ações encobertas em ambiente digital cada vez mais frequentes.

Ora, uma vez que esta deslocação do crime do ambiente físico para o ambiente digital, potenciada pelo aparecimento das novas tecnologias, é relativamente recente, é possível afirmar que as várias disposições legais atinentes à matéria probatória, mormente as existentes no Regime Jurídico das Ações Encobertas, relevante para o estudo em apreço, se encontram equacionadas e desenhadas para a obtenção e recolha de prova num plano visível e tangível. Tal como explica David Silva Ramalho, "*Os meios de obtenção de prova previstos na lei, tal como se encontram regulados, são, portanto, o resultado de uma evolução jurídica testada empiricamente no ambiente físico para o qual foram concebidos. (...) Independentemente do fim, interesse ou direito que cada norma processual visa tutelar ou do trajeto evolutivo que seguiu, a verdade é que, pelo menos aquelas que existem há mais de duas décadas, estão concebidas para uma realidade que não contempla o mundo digital.*"[288].

As ações encobertas, enquanto meio de obtenção de prova, visam, por excelência, ganhar a confiança dos autores da prática de crimes para proceder à recolha de prova que, de outra forma, se veria dificultada, ou até mesmo impossibilitada. Esta recolha de prova será, necessariamente, operada de forma diferente, caso estejamos perante uma ação encoberta em ambiente físico ou, pelo contrário, se a mesma decorrer num plano virtual ou digital. A realização de ações encobertas em ambiente físico encontra-se já devidamente acautelada e regulamentada pela Lei n.º 101/2001, mas e o que dizer relativamente às ações encobertas em ambiente digital?

[288] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, pp. 240-241.

Depois de uma extensa e detalhada análise à legislação portuguesa em vigor, foi possível concluir que inexiste um qualquer regime jurídico especificamente destinado à regulamentação do recurso às ações encobertas em ambiente digital – tão só encontramos o artigo 19.º da Lei do Cibercrime, que se limita a remeter para o *supra* mencionado Regime Jurídico das Ações Encobertas, a alargar o catálogo de crimes cuja investigação criminal se pode socorrer de uma ação encoberta e, mais uma vez, a remeter para outros diplomas legais, desta feita para as normas previstas no Código de Processo Penal relativas à interceção de comunicações, quando seja necessário recorrer a meios e dispositivos informáticos[289].

A inexistência de um regime jurídico expresso resulta na aplicação, por remissão e analogia, do regime jurídico atualmente vigente, isto é, a Lei n.º 101/2001 – um texto normativo claramente pensado para as ações encobertas em ambiente físico. Esta aplicação de um regime equacionado para lidar com características palpáveis a realidades com traços unicamente digitais é apenas mais um exemplo da tendência a que temos vindo a assistir nas últimas décadas no seio da aplicação normativa portuguesa. Com efeito, "*O lastro histórico do nosso sistema processual penal e a tendencial reduzida literacia informática dos juristas, tendem a relegar as inovações tecnológicas para o domínio da analogia, testando os seus limites até ao ponto em que a própria compreensão da realidade tem de ser adaptada ao Direito, e não o inverso*."[290].

E é precisamente sobre esta consideração que é necessário indagar: será que não deveria efetivamente ser o Direito a adaptar-se à realidade? Será que esta adaptação da realidade ao Direito e consequente aplicação do Regime Jurídico das Ações Encobertas cumpre a importante exigência de tutela do meio informático? Ou será que a realidade e o mundo digital deveriam ter uma tutela exclusivamente desenhada para si? Podemos dizer que as especificidades do mundo digital já se encontram, nos dias de hoje, suficientemente acauteladas? Direitos fundamentais como o direito à autodeterminação informacional ou o direito à integridade e confidencialidade dos sistemas informáticos encontram-se atualmente salvaguardados?

---

[289] Cfr. artigo 19.º da Lei do Cibercrime:
"*1 - É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:*
a) Os previstos na presente lei;
b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, 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.
2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.";
[290] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 241;

Pretendemos, neste capítulo, encontrar a resposta a estas questões e chegar ao verdadeiro cerne do presente estudo – compreender se existe, ou não, a emergência da criação de um novo regime jurídico dedicado, em exclusivo, às ações encobertas em ambiente digital e ao recurso às mesmas.

4.1. Especificidades das ações encobertas em ambiente digital

Para que seja possível compreender se existe a necessidade de criação de um regime jurídico específico para as ações encobertas em ambiente digital, torna-se necessário, em primeiro lugar, entender quais as características e aspetos específicos que estas apresentam e que são merecedores de uma tutela efetiva. De entre as várias especificidades estudadas no âmbito do presente estudo, iremos analisar as seguintes: adoção de múltiplas identidades; a existência de um risco diminuído para o agente encoberto; a necessidade de recursos físicos adequados, nomeadamente a utilização de computadores designados para esse efeitos e a proteção de ligações à *internet*; a necessidade de conhecimentos técnicos por parte do agente encoberto e o consequente possível aproveitamento destes; a necessidade de controlo acrescido e registo permanente de toda a ação encoberta; e, ainda, o recurso a *chatbots*.

No seio de uma ação encoberta em ambiente físico, pode ser atribuída ao agente encoberto, nos termos do disposto no artigo 5.º do Regime Jurídico das Ações Encobertas, uma identidade fictícia, que este usará para se infiltrar numa determinada organização ou grupo criminoso. Quando a ação encoberta decorre no ambiente digital, não existe uma presença física do agente encoberto, isto é, ao passo que na ação encoberta em ambiente físico o agente encoberto interage pessoalmente com os visados e, como tal, ao mesmo só pode ser atribuída uma identidade, na ação encoberta em ambiente digital tal não sucede. Uma vez que o agente encoberto se encontra sentando atrás de um computador, este pode ter uma qualquer identidade que não coadune necessariamente com os seus atributos físicos e múltiplas identidades ao mesmo tempo. Como salienta Gemma Davies, "*Online undercover operations require a significant degree of skill as officers must learn to mimic the patterns and style of online personas they are impersonating and this represents a significant investment of time and resources for LEAs. One of the main priorities of undercover LEAs (Law Enforcement Agencies) is investigating chat rooms, newsgroups, and peer-to-peer networks. Agents enter forums posing as offenders requesting*

images from others, or they enter groups posing as children to lure out the pedophiles in the group."[291].

Com efeito, nas ações encobertas em ambiente digital, o agente encoberto pode, por exemplo, participar em várias salas de *chat* ao mesmo tempo, atuando com várias identidades distintas numa mesma sala; ou pode suceder de o agente encoberto sair de uma determinada sala de *chat* em que se apresentava com uma identidade e retornar segundos depois com uma outra identidade totalmente distinta; ou pode, ainda, existir situações em que o agente encoberto adota uma identidade de uma pessoa com a aparência de alguém já conhecido e próximo do visado pela ação encoberta[292]. De igual modo relevante no que respeita à adoção de identidades nas ações encobertas em ambiente digital é o facto de poder ser necessário criar vários perfis, conexos ao perfil da identidade fictícia do agente encoberto, para dar credibilidade a este, como seja o caso de perfis de familiares ou amigos.

Uma outra especificidade das ações encobertas em ambiente digital é a existência de um risco diminuto para o agente encoberto, quando comparado com o risco suportado por um agente encoberto numa ação realizada em ambiente físico. Tendo em conta que não se expõe fisicamente e que não existe um contacto pessoal com o visado por este meio oculto de investigação criminal, o agente encoberto pode exercer a sua atividade a partir do seu local de trabalho ou, até mesmo, a partir de sua casa. Esta ausência de exposição física permite uma interação com outros indivíduos a uma escala muito maior do que aquela possível no ambiente físico e dá ao agente encoberto uma amplitude para falhar, isto é, caso o agente encoberto cometa algum erro, tal não se consubstanciará em grandes consequências para a sua segurança, como ocorre no ambiente físico[293].

Neste sentido, é ainda importante a conclusão avançada pelo *Department of Justice* dos Estados Unidos da América, de acordo com a qual: "*Some of the restrictions on attending physical-world meetings, however, may not apply to the online environment. In the physical world, agencies must be concerned that an agente appearing in person may be recognized; that fact, in turn, may cause other participants to believe, rightly or wrongly, that they are under investigation (...). Although many online chat facilities allow participants to know who else is present in the forum, the available information (often only a user-selected nickname) generally does not reveal a participant's real-world identity. In determining whether to permit an agent to attend a public*

[291] DAVIES, Gemma, "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers", *In: The Journal of Criminal Law*, Vol. 84(5), 2020, pp. 411, disponível em https://bityli.com/bDPGg, último acesso em 14-02-2022;
[292] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, pp. 284-285;
[293] *Idem*, p. 285.

meeting online, the agency must recognize that these important differences may support allowing an agent to observe an online meeting where the agency would be reluctant to allow the agent to appear if a physical-world meeting were held on the same topic."[294].

Não obstante o agente encoberto em ambiente digital não corra um risco tão elevado como o agente encoberto em ambiente físico, devem ser, igualmente, assegurados ao primeiro, todos os meios físicos e informáticos necessários e imprescindíveis à realização e sucesso da ação encoberta, nomeadamente computador e ligação segura e protegida à *internet*. Não pode ser permitido ao agente encoberto utilizar o seu computador pessoal ou utilizar uma ligação à *internet*, na qual constem os seus dados pessoais, porquanto tal pode ter graves consequências no decorrer da investigação criminal em apreço, mormente ao nível da integridade da cadeia de custódia da prova. Com efeito, se o agente encoberto utilizar o seu computador pessoal para realização da ação encoberta, ou se utilizar um computador designado pelo Órgão de Polícia Criminal, mas neste visitar websites ou efetuar pesquisas de caráter pessoal, pode tornar complicada a tarefa de manter intacta a cadeia de custódia de prova, dado que o uso pessoal que o agente encoberto faz do computador pode contaminar todos os indícios de atividade criminosa detetados. Nas palavras de Manuel Magriço, "*Sobretudo nas investigações encobertas em linha, em que há necessidade de utilizar um computador e ligação à Internet, é fator de risco elevado utilizá-lo para enviar mensagens de correio eletrónico privadas, aceder ao sistema de 'homebanking', efetuar pesquisas e, inclusive, ver pornografia, pois tais atividades podem ser facilmente detetadas pelos suspeitos e colocar em causa a credibilidade do investigador e da prova recolhida.*"[295].

Numa outra perspetiva, utilizar uma ligação segura à *internet* é igualmente importante para garantir que os suspeitos alvo da ação encoberta em apreço não obtêm informações acerca da identidade real do agente encoberto, sendo, neste aspeto, necessário garantir que não seja possível obter, através de qualquer empresa fornecedora de serviços de *internet* , dados que possam levar a uma identificação do agente em apreço[296] [297].

---

[294] DEPARTMENT OF JUSTICE, *Online Investigative Principles for Federal Law Enforcement Agents*, 1999, p. 23, disponível em https://bityli.com/LhlWr, último acesso em 16-02-2022;

[295] MAGRIÇO, Manuel Eduardo Aires, *A Exploração Sexual de Crianças no Ciberespaço – Aquisição e Valoração de Prova Forense de Natureza Digital*, Sinapis Editores, 2013, p. 145;

[296] *Idem*, pp. 146-147;

[297] No mesmo sentido, vide SHIPLEY, Todd G., BOWKER, Art, Investigating Internet Crimes – An Introduction to Solving Crimes in Cyberspace, Elsevier, 2014, p. 250: "*First, the equipment should only be used for undercover operations. Accessing the Internet for an agency or a company owned system may reveal your real identity. Personal information and/or agency or company information should never be stored on the undercover computer. This prevents the possibility of an adversary identifying your true identity if they offensively work back to your computer. The computer should not be connected to any network system within the agency or company. The investigator should plan for and prepare for the possibility that the undercover system could be accessed by a target while you are connected to the Internet.*".

Tendo a ação encoberta lugar no ambiente digital, não basta que o agente encoberto apresente as características necessárias à realização de uma, dita normal, ação encoberta. É necessário que a estas se somem conhecimentos técnicos e informáticos específicos, que não se confundem com os adquiridos ou possuídos ao nível do utilizador frequente[298]. Conhecimentos estes que implicam, não só a familiarização com os mecanismos de ocultação de identidade *online* a adotar, mas também com as diferentes ferramentas adotadas pelos meliantes para se escaparem à atividade de monitorização e deteção levada a cabo pelas autoridades policiais nas respetivas investigações criminais. Inexistindo estes conhecimentos informáticos, a ação encoberta em ambiente digital está claramente votada ao insucesso, porquanto os visados por este meio oculto de obtenção de prova poderiam chegar facilmente à verdadeira identidade do agente em apreço, deitando por terra toda a ação encoberta, bem como o que se pretendia alcançar com a mesma.

Sucede que, como ressalva David Ramalho, "*Esta segurança adicional, aliada ao conhecimento técnico que o agente encoberto em ambiente digital deverá ter, traz, porém, um risco de dimensão idêntica: o do aproveitamento, por parte do agente encoberto, do acesso privilegiado ao visado e das tecnologias anti forenses à sua disposição para benefício próprio (...) ou em benefício ilícito da investigação (...).*"[299]. Um agente encoberto em ambiente digital deve apresentar, como já referido *supra*, especiais conhecimentos tecnológicos e informáticos, nos quais se incluem também ferramentas cujo propósito é eliminar quaisquer vestígios da presença do agente *online*. Ora, como rapidamente se conclui, apesar de, na grande maioria dos casos, estas ferramentas serem utilizadas no melhor interesse da investigação criminal em curso, situações também as há em que o recurso às mesmas é efetuado à revelia da investigação e no interesse do próprio agente encoberto, que se pretende locupletar às custas desta.

Um exemplo deste perigo que advém dos conhecimentos informáticos possuídos pelo agente encoberto é o celebre caso *Silk Road*. Em Janeiro de 2011, surgiu na *Dark Web*, um *website* denominado de *Silk Road*, que tratava de um mercado digital de drogas, identificações falsas, serviços de *hacking*, entre outros. Este website teve uma grande visibilidade porquanto combinava duas tecnologias de anonimização que tornavam praticamente indetetável a localização dos servidores em que se encontrava alojado o *Silk Road* e os seus utilizadores e permitia que as transações efetuadas não pudessem ser conhecidas por outros que não os seus intervenientes,

[298] MATA, Federico Bueno de, "El Agente Encubierto en Internet: Mentiras Virtuales para Alcanzar la Justicia", s/d, p. 301, disponível em https://bityli.com/vduXB, último acesso em 22-02-2022;
[299] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 286;

através da utilização da criptomoeda Bitcoin[300]. O *website Silk Road* era administrado pelo autointitulado *Dread Pirate Roberts*, cuja identidade à data se desconhecia. Face à *supra* mencionada dificuldade de localizar os servidores em que se encontram alojados não só o *Silk Road*, como também os seus utilizadores, começaram a ser desenvolvidas inúmeras ações encobertas, numa das quais um agente da *Drug Enforcement Administration*, Carl Force IV, fez-se passar por um traficante de droga e ganhou a confiança do *Dread Pirate Roberts* e de outros membros da administração do *website*. Em Junho de 2013, após várias tentativas, foi possível localizar os servidores do *Silk Road* na Islândia e, posteriormente, Ross Ulbricht foi identificado como o *Dread Pirate Roberts*, o cérebro por detrás de todo o esquema, tendo este sido condenado, em Maio de 2015, a prisão perpétua sem possibilidade de liberdade condicional[301]. Ainda antes de ser proferida uma decisão relativamente a Ross Ulbricht, foi deduzida uma queixa contra o agente da *Drug Enforcement Administration*, Carl Force IV, e contra o agente dos serviços secretos Shaun Bridges, por suspeita da prática dos crimes de fraude, suborno, extorsão e abuso de confiança, praticados no decorrer das ações encobertas levadas a cabo pela investigação ao *website Silk Road*. O agente Carl Force IV "*(...) terá criado outras identidades fictícias não autorizadas, através das quais comunicava com Dread Pirate Roberts e o extorquia em troca da promessa de não revelação de dados às autoridades ou vendera informações da investigação a troco de cerca de $100,000,00, os quais foram efetivamente pagos.*"[302], tendo sido condenado a seis anos e meio de prisão; já o agente Shaun Bridges terá aproveitado o acesso de que dispunha ao *Silk Road* para se apropriar de uma elevada quantia em *bitcoins*, o que resultou numa condenação de 6 anos, tendo esta sido posteriormente aumentada para 8 anos, em virtude de Bridges ter tentado mover e lavar *bitcoins* guardadas[303].

Através da análise do exemplo vindo de expor, podemos afirmar que o agente encoberto em ambiente digital dispõe de um enorme poder, dado possuir conhecimentos técnicos específicos, que a generalidade das pessoas não consegue sequer compreender. Tal circunstância dá ao agente encoberto uma maior margem para encobrir possíveis erros ou, até mesmo,

---

[300] Nesta senda, vide SHIPLEY, Todd G., BOWKER, Art, *Investigating Internet Crimes – An Introduction to Solving Crimes in Cyberspace*, Elsevier, 2014, p. 243: "*In 2009, Satoshi Nakamoto, an anonymous (as in a hacker pseudonym not part of the hacker group anonymous) hacker created a digital peer to peer currency that is not backed by any government. This digital currency, known as Bitcoin, is automatically "mined" on a set schedule using Bitcoin user's computers around the world. Basically, the user's computers are running a program that creates the digital currency. The exchange of this currency is all controlled by computer and it can't be traced. The amount to be mined is set at 21 million. What is the big deal? It after all is not "real." Well, the currency is being used to actually buy things in the real world, and there are actually sites that have set up na exchange rate for Bitcoins to dollars, to pounds, etc.*";

[301] Toda a informação relativa a este caso disponível em https://bityli.com/cbwfC, último acesso em 22-02-2022;

[302] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 33;

[303] De acordo com o The United States Department of Justice, "*Bridges admitted to using a private key to access a digital wallet belonging to the U.S. government, and subsequently transferring the bitcoin to other digital wallets at other bitcoin exchanges to which only he had access. As part of his plea, Bridges agreed to turn over the stolen bitcoin to U.S. agents.*", disponível em https://bityli.com/qRBLn, último acesso em 22-02-2022.

defraudar toda a investigação criminal sem que ninguém se aperceba disso. Tendo em conta esta possibilidade, é absolutamente necessário que o controlo exercido sobre o agente e sobre a própria investigação em apreço seja superior ao habitual, precisamente para evitar situações idênticas às do caso *Silk Road*, devendo a pessoa encarregada deste supervisionamento ser dotada dos conhecimentos necessários ou, em alternativa, ter acesso a alguém que os possua. Uma das formas de controlo que deve existir é o registo permanente de todas as atividades realizadas e atos empreendidos no seio da ação encoberta em ambiente digital. Encontrando-se tudo registado, não só é possível demonstrar claramente todos os passos percorridos durante a ação encoberta para chegar ao resultado final, como também afasta qualquer tipo de dúvida que possa surgir acerca da validade e admissibilidade da prova recolhida[304].

Por último, cumpre, ainda, abordar uma possibilidade que o ambiente digital pode trazer para a realização de ações encobertas no mesmo. O aparecimento das novas tecnologias e o avanço e rápido desenvolvimento das mesmas trouxe consigo a Inteligência Artificial, o mesmo é dizer "*(...) a capacidade que uma máquina tem para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade*."[305], e, consequentemente, o recurso a *chatbots*. Um *chatbot* é um programa informático, criado através de inteligência artificial, que simula conversas e interações humanas, escritas ou faladas, permitindo que seres humanos interajam com dispositivos digitais como se estivessem a comunicar com uma pessoa real[306]. Nas ações encobertas realizadas no ambiente digital, não existe qualquer contacto físico entre o agente encoberto e o visado, apenas ocorrem conversas através de perfis criados nas mais variadas redes sociais ou *websites*. O visado pela ação encoberta não sabe qual é a verdadeira aparência da pessoa com quem se encontra a falar, daí que se discuta a possibilidade do recurso a *chatbots*, que desempenhariam a mesma função que o agente encoberto, mas com um maior alcance.

Não nos querendo debruçar, neste momento, sobre as teorias a favor ou contra a utilização deste tipo de ferramenta informática que possam ser formuladas, importa atentar no caso do *chatbot Sweetie*. Em 2013, a organização não governamental *Terre des Hommes*, com sede na Holanda, criou o programa *Sweetie 1.0*, uma menina virtual, de nome *Sweetie*, com 10 anos de idade e de nacionalidade filipina. Com o objetivo de reunir o máximo de informação sobre indivíduos que, através da *internet*, entravam em contacto com a menina virtual e a aliciavam para

[304] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019, p. 286;
[305] Informação disponível em https://bityli.com/zhEdD, último acesso em 24-02-2022;
[306] Informação disponível em https://bityli.com/uibLj, último acesso em 24-02-2022.

atividades de cariz sexual, a *Sweetie* era gerida por um membro da organização que desenvolvia as conversas com os referidos indivíduos em salas de *chat* públicas. O programa *Sweetie 1.0* apresentou resultados de tamanha escala que, em 2015, a *Terre des Hommes* e uma equipa de especialistas encetaram esforços para desenvolver uma melhor versão, tendo surgido a *Sweetie 2.0*. Esta nova versão é operada por recurso à inteligência artificial, tratando-se agora de um *chatbot* que desenvolve várias conversas com vários indivíduos, ao mesmo tempo[307]. Países como a Bélgica, Dinamarca, Holanda, Inglaterra e Austrália já utilizam o programa em apreço e, apesar de, como referimos *supra*, não ser consensual, a verdade é que se trata de uma realidade que o ambiente digital impõe que se considere e estude.

4.2. Insuficiência da aplicação, por remissão ou analogia, do regime jurídico das ações encobertas vigente

Como já tivemos oportunidade de referir *supra*, da análise efetuada no âmbito do presente estudo resultou que inexiste, na legislação portuguesa em vigor, um qualquer regime jurídico especificamente destinado à regulamentação do recurso às ações encobertas em ambiente digital. Estas apenas são abordadas, de forma mais concreta, no artigo 19.º da Lei do Cibercrime, que se limita a remeter para a aplicação do Regime Jurídico das Ações Encobertas; a alargar o catálogo de crimes cuja investigação criminal se pode socorrer de uma ação encoberta e, mais uma vez, a remeter para outros diplomas legais, desta feita para as normas previstas no Código de Processo Penal relativas à interceção de comunicações, quando seja necessário recorrer a meios e dispositivos informáticos. Desta forma, sendo necessário acautelar alguma situação atinente a uma ação encoberta realizada em ambiente digital, deverá ter-se em linha de conta o referido preceito legal constante da Lei do Cibercrime, as normas relativas à interceção de comunicações e, em caso de insuficiência das mesmas, aplicar-se-á, por remissão ou analogia, o Regime Jurídico das Ações Encobertas, previsto na Lei n.º 101/2001.

Da análise do artigo 19.º da Lei do Cibercrime, é possível observar que estamos perante uma norma remissiva. Ora, as normas remissivas traduzem-se naquelas em que o legislador, ao invés de regulamentar especificamente uma questão de direito, indicam que à mesma se apliquem outras normas jurídicas, integrantes do mesmo ou de outro diploma legal. A remissão consiste, assim, num instrumento de técnica legislativa ao qual se recorre sempre que um determinado

[307] Informação disponível em https://bityli.com/InlbR, último acesso em 24-02-2022;

instituto jurídico possui já a sua devida regulamentação e o legislador pretende que esta se aplique a um outro instituto ou facto jurídico. Existem dois tipos distintos de remissão, a saber: a estática ou material; e a dinâmica ou formal, de acordo com a qual se remete para uma determinada norma, atendendo ao facto de, num certo momento, esta regular uma matéria em causa, ainda que posteriormente o conteúdo desta sofra alterações – este último é o tipo de remissão utilizado com mais frequência[308].

Importa, nesta senda, distinguir a aplicação de um determinado regime jurídico por remissão da aplicação por analogia. A aplicação por analogia surge quando estamos perante uma lacuna do Direito, um caso para o qual ainda não existe solução legal. Nestes casos, temos que procurar no Direito uma norma que regule um outro caso diferente, mas que seja análogo ao que se pretende agora acautelar. Deve ser feito, pelo intérprete, um exercício de compreender se o legislador, caso tivesse previsto o caso omisso, o regularia da mesma forma ou de forma semelhante ao que fez para o caso análogo[309]. Desta forma, Desta forma, a analogia traduz-se na comparação de um caso concreto com outro, pretendendo-se com a mesma identificar as suas diferenças e semelhanças e, bem assim, compreender se as estas detêm relevância suficiente para que se possa enquadrar o caso omisso na estatuição da norma relativa ao caso análogo.

Ora, o artigo 19.º da Lei do Cibercrime não só remete para a aplicação do Regime Jurídico das Ações Encobertas, previsto na Lei n.º 101/2001, como se pode subentender, da sua leitura, que, no caso de uma ação encoberta em ambiente digital se deverá aplicar, na falta de um regime específico, e, bem assim, por analogia, o referido Regime Jurídico das Ações Encobertas. Sucede que, no nosso humilde entendimento, este regime jurídico não é, de todo, adequado a garantir a tutela efetiva dos bens jurídicos afetados pelo recurso ao meio oculto de obtenção de prova que são as ações encobertas em ambiente digital.

Com efeito, o Regime Jurídico das Ações Encobertas não aborda, em qualquer um dos seus preceitos legais, a possibilidade de o agente encoberto em ambiente digital adotar múltiplas identidades, em virtude de não ter que dar a conhecer a sua verdadeira imagem e características físicas, tal como sucede nas ações encobertas realizadas no mundo físico. O artigo 5.º da Lei n.º 101/2001, sob a epígrafe *Identidade Fictícia*, determina que os agentes de polícia criminal podem atuar sob uma identidade fictícia, que lhes é atribuída por despacho do Ministério da Justiça, sendo a mesma válida por um período de seis meses, prorrogáveis por períodos de igual duração. Esta

[308] Neste sentido, vide Parecer do Conselho Consultivo da Procuradoria da República Portuguesa, com o n.º PGRP00003069, datado de 01-03-2010, disponível em https://bityli.com/oMDnu, último acesso em 02-03-2022;
[309] SILVA, Germano Marques da, *Introdução ao Estudo do Direito*, 5ª edição, Universidade Católica Editora, 2015, pp. 278-279;

norma não acautela situações em que, por exemplo, seja necessário recorrer a um terceiro, para atuar como agente encoberto, em virtude das suas capacidades e conhecimentos técnicos, dado que a norma determina que apenas os agentes de polícia criminal podem adotar identidades fictícias. Mais, ao referir que ao agente de polícia criminal é atribuída uma identidade fictícia, válida por um período de seis meses, a norma exclui a adoção de mais do que uma identidade – o que no ambiente digital pode ser fundamental para o sucesso da ação encoberta. De igual modo, tendo em conta a ausência de contacto físico característica do ambiente digital e a possibilidade de adoção de um perfil com uma qualquer aparência, a norma é totalmente alheia e, bem assim, inaplicável às situações em que se queira criar um perfil *online* com a aparência física de alguém conhecido ou próximo do visado pela ação encoberta. O entendimento que se sustenta é igualmente aplicável aos casos em que seja necessário criar perfis conexos ao perfil principal do agente encoberto para aumentar a credibilidade deste último.

Uma questão também não abordada pelo Regime Jurídicos das Ações Encobertas é os requisitos que determinada pessoa deve possuir para poder atuar como agente encoberto. O n.º 1 do artigo 1.º do referido diploma legal refere que as ações encobertas podem ser desenvolvidas por funcionários de investigação criminal ou terceiros que atuam sob o controlo da Polícia Judiciária, sendo que, nos termos do n.º 2 do artigo 3.º, ninguém poderá ser obrigado a participar numa ação encoberta. Como já se deixou explanado *supra*, para que uma ação encoberta em ambiente digital possa ter sucesso, é essencial a pessoa a infiltrar disponha de um conjunto de elevados conhecimentos técnicos e informáticos, que em nada se identificam com os conhecimentos adquiridos por um qualquer utilizador da *internet*. Atualmente, o Regime Jurídico das Ações Encobertas não se refere, em nenhum artigo, a quais as características que devem ser valoradas aquando da escolha do agente encoberto em ambiente físico, quanto mais se debruça sobre esta questão da necessidade de conhecimentos específicos. Da aplicação deste regime jurídico a uma ação encoberta em ambiente digital pode resultar a escolha de um agente que não possua os devidos conhecimentos, já que nada é exigido nos termos do mesmo. Esta falta de conhecimentos pode ter consequências gravíssimas, mormente ao nível da segurança do agente encoberto que, não se encontrando familiarizado com os mecanismos de ocultação de identidade em linha, pode ver a sua verdadeira identidade descoberta pelo visado da ação encoberta, colocando assim em perigo não só a vida do agente como das pessoas mais próximas de si.

Esta necessidade de exigência de conhecimentos técnicos adicionais para a realização de ações encobertas em ambiente digital traz consigo uma outra insuficiência do Regime Jurídico das

Ações Encobertas – a junção do relatório do agente encoberto apenas quando tal se reputar como indispensável. Com efeito, sendo imperativo que o agente encoberto possua conhecimentos informáticos avançados, pode acontecer que o mesmo se aproveite deles e ludibrie a investigação criminal em curso para seu benefício. Isto porque, atualmente podemos dizer que quase todas as pessoas possuem conhecimentos informáticos ao nível do utilizador frequente; mas, ainda são relativamente raras aquelas que possuem conhecimentos profundos da internet e de todos os mecanismos necessários para a ocultação de identidade em linha e recolha de prova digital. Tal circunstância faz com que o agente encoberto em ambiente digital tenha uma maior liberdade do que a do agente encoberto em ambiente físico e esta liberdade deve ser devidamente acautelada e controlada por parte das autoridades que supervisionam a realização da ação encoberta. Nesta senda, não basta que, conforme resulta do n.º 1 do artigo 4 do Regime Jurídico das Ações Encobertas[310], o relatório do agente encoberto apenas seja junto ao processo em caso de se reputar absolutamente indispensável em termos probatórios. No nosso entendimento, o relatório do agente encoberto em ambiente digital deve ser sempre junto aos autos, ressalvando-se sempre a identidade do respetivo agente por claros motivos de segurança. Com esta junção, será muito mais fácil atestar e sindicar a legalidade e admissibilidade dos procedimentos levados a cabo.

Por último, e porventura a mais evidente das insuficiências do Regime Jurídico das Ações Encobertas, diz respeito à regulamentação dos recursos a utilizar na âmbito das ações encobertas em ambiente digital, sejam eles físicos ou informáticos. Da análise do referido diploma legal resulta que inexiste qualquer tipo de norma atinente aos meios físicos que devem ser assegurados ao agente encoberto, nomeadamente um computador estritamente adstrito às ações encoberta a realizar. Como vimos *supra*, uma utilização indevida do computador utilizado na ação encoberta ou a utilização de um computador que não pertencente ao órgão de polícia criminal pode destruir por completo a integridade da cadeia de prova[311]. De igual modo, a inexistência de uma ligação segura e protegida à *internet* pode resultar em graves consequências para o desfecho da investigação criminal e, ainda, para a segurança do agente encoberto. Por outro lado, sabemos também que a *internet* trouxe consigo inúmeras possibilidades anteriormente inexistentes, como seja o recurso à Inteligência Artificial, que se pode revelar como extremamente útil para as ações

[310] Vide artigo 4.º, n.º 1: "*A autoridade judiciária só ordenará a junção ao processo do relato a que se refere o n.º 5 do artigo 3.º se a reputar absolutamente indispensável em termos probatórios.*".

[311] Vide, neste sentido, VALENTE, Manuel Monteiro Guedes, Cadeia de Custódia da Prova, Almedina, 2019, p. 46: "*Desta feita, todo o procedimento da cadeia de custódia da prova está obrigado a respeitar e a promover os princípios constitucionais processuais penais inatos ao instituto da prova, cuja violação vicia a sua utilização o processo: v. g., exige a sua 'inutilização' em sede de audiência de discussão e julgamento por ter ferido a impenetrabilidade da identidade (originalidade) e da autenticidade (integralidade) da prova por ter havido uma ausência de controlo judicial e violação dos deveres de cuidado impostos àqueles que devem zelar pela garantia e tutela da identidade e da autenticidade da prova por meio da cadeia de custódia da prova.*";

encobertas em ambiente digital, aumentando, de forma exponencial, a eficácia destas. Daí que seja necessário regulamentar e acautelar estas situações, coisa que é totalmente alheia ao Regime Jurídico das Ações Encobertas.

Do vindo de expor, resulta claramente que o Regime Jurídico das Ações Encobertas não aborda suficientemente ou não se pronuncia de todo sobre questões de elevada importância no que respeita às ações encobertas em ambiente digital. Tal implica que não exista uma tutela eficaz dos direitos fundamentais afetados por este meio oculto de investigação criminal e recolha de prova, o que não se pode conceder.

Cumpre, ainda, atentar que o artigo 19.º da Lei da Cibercrime remete também para as regras relativas à interceção de comunicações, quando seja necessário o recurso a meios e dispositivos informáticos, previsto no artigo 18.º. De acordo com este artigo, a interceção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho que autoriza a diligência de prova especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação. O n.º 4 do artigo 18.º determina que "*Em tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.*". Ora, da análise destes artigos do Código de Processo Penal é possível verificar que as insuficiências acima expostas relativamente à utilização de meios e dispositivos informáticos no seio das ações encobertas em ambiente digital em nada resultam acuteladas. Isto é, em nada se regulamenta a qualidade dos meios informáticos a utilizar, como os utilizar ou ainda, a possibilidade de recurso à Inteligência Artificial.

De toda a investigação encetada no âmbito do presente estudo, é evidente que o regime jurídico em vigor e atualmente aplicável às ações encobertas em ambiente digital é manifestamente insuficiente, sendo, por isso, urgente a criação de um novo regime jurídico especificamente criado para tutelar este meio de obtenção de prova.

4.3. Esboço de um novo regime jurídico

A constante evolução da criminalidade, especialmente da criminalidade organizada, potenciada pelo aparecimento das novas tecnologias, e a deslocação da prática dos factos ilícitos para o ambiente digital fez crescer a necessidade de recorrer a meios ocultos de obtenção de prova, mormente às ações encobertas em ambiente digital. Face ao *supra* exposto, torna-se claro

que o regime jurídico atualmente vigente para as ações encobertas em ambiente digital, resultante de uma conjugação entre o Regime Jurídico das Ações Encobertas, a Lei do Cibercrime e as disposições legais relativas à interceção de comunicações, não é, de todo, suficiente para acautelar os direitos fundamentais restringidos pela realização de uma ação encoberta no âmbito de uma investigação criminal. Nesta senda, urge criar um novo regime jurídico que seja especificamente desenhado para o efeito e tenha em conta todas os traços característicos das ações encobertas em ambiente digital.

Uma das primeiras questões que se impõe aquando de equacionar um novo regime jurídico dedicado às ações encobertas em ambiente digital prende-se com saber a quem compete proceder à criação do mesmo. A competência legislativa e, consequentemente, a reserva de lei, encontram-se previstas nos artigos 164.º e 165.º da Constituição da República Portuguesa. Ora, a reserva de lei traduz-se na delimitação de um determinado conjunto de matérias que devem ser regulados por lei, isto é, "*(...) existe reserva de lei quando a constituição prescreve que o regime jurídico de determinada matéria seja regulado por lei e só por lei, com exclusão de outras fontes normativas*."[312]. Esta reserva de lei pode ser absoluta – caso todos os atos legislativos referentes a determinada matéria tenham de ser leis emanadas pela Assembleia da República – ou pode ser relativa – quando, relativamente a certas matérias, a Assembleia da República pode autorizar o governo a legislar sobre as mesmas, desta feita sobre a forma de decreto-lei autorizado[313]. Com a realização de ações encobertas em ambiente digital existe um recurso a meios ocultos de obtenção de prova e de investigação criminal, recurso este que provoca inevitavelmente restrições de direitos fundamentais, mormente direitos, liberdades e garantias. De acordo com a alínea b) do n.º 1 do artigo 165.º da Constituição da República Portuguesa, é da exclusiva competência da Assembleia da República legislar, salvo autorização ao Governo, sobre direitos, liberdades e garantias. Assim, sendo as ações encobertas em ambiente digital um meio oculto de obtenção de prova que provoca grandes restrições de direitos fundamentais, deve o novo regime jurídico a ser criado emanar de uma lei da Assembleia da República ou de um decreto-lei autorizado do governo.

De igual modo importante no processo de criação de um novo regime jurídico é o respeito pelo princípio da proporcionalidade, princípio este que "*(...) tem inscrito uma função de controlo que emerge sempre que a proteção de interesses públicos possa entrar em conflito com os direitos fundamentais e liberdades públicas dos cidadãos, o que no âmbito penal ocorre com*

[312] CANOTILHO, J. Gomes, *Direito Constitucional e Teoria da Constituição*, 7ª Edição, Coimbra, Almedina, 2003, p. 724;
[313] CANOTILHO, J. Gomes, e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume II, 4ª edição, Coimbra Editora, 2010, pp. 308-324.

frequência."[314]. O princípio da proporcionalidade pode dividir-se em três diferentes vertentes, a saber: princípio da adequação ou idoneidade; princípio da necessidade ou exigibilidade; e princípio da proporcionalidade em sentido restrito. Nos termos do princípio da adequação, uma qualquer medida restritiva de direitos, liberdades e garantias deve apresentar-se como adequada para prosseguir os fins visados pela mesma[315]. Assim, as ações encobertas em ambiente digital apenas poderiam ter lugar quando existisse uma importância investigatória de elevadas dimensões e quando fosse possível obter com a mesma elementos de prova efetivamente necessário para a investigação criminal em curso.

Por seu turno, o princípio da necessidade determina que a medida restritiva de direitos fundamentais a adotar deve revelar-se como estritamente necessária, isto é, os resultados pretendidos não poderiam ter sido obtidos através de uma qualquer outra medida que se mostrasse menos onerosa para os direitos, liberdades e garantias dos cidadãos[316]. Nesta senda, para que se possa recorrer a uma ação encoberta em ambiente digital, é imperativo que exista uma grande dificuldade de obtenção de prova no seio da investigação criminal, de tal modo que não seria possível chegar à descoberta da verdade ou à obtenção de prova sem a mesma.

Finalmente, mas não menos importante, o princípio da proporcionalidade em sentido restrito impõe que a medida restritiva adotada e os fins obtidos se situem numa justa medida, impedindo, assim, que ocorram casos em que a aplicação da referida medida implique uma restrição de direitos, liberdades e garantias excessivamente desproporcional[317]. Deste modo, apenas se poderá recorrer às ações encobertas em ambiente digital quando estiver em causa a investigação de criminalidade organizada e somente pela prática dos crimes previstos nos artigos 3.º a 8.º da Lei do Cibercrime, bem como os equacionados na alínea b) do n.º 1 do artigo 19.º do referido diploma legal[318] e nas alíneas i) a m) do artigo 1.º do Código de Processo Penal, quando perpetrados por meio de dispositivos informáticos.

Uma outra temática a ter em consideração diz respeito a quem compete autorizar a realização das ações encobertas em ambiente digital. No regime jurídico atualmente em vigor, tal autorização compete, nos termos dos n.º 3 e 4 do artigo 3.º do Regime Jurídico das Ações

---

[314] Vide Acórdão do Supremo Tribunal de Justiça, datado de 31-03-2011, relativo ao processo n.º 257/10.9YRCBR.S1, disponível em https://bityli.com/xWJBG, último acesso em 21-03-2022;
[315] CANOTILHO, J. Gomes, e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume II, 4ª edição, Coimbra Editora, 2010, p. 392;
[316] *Ibidem*;
[317] *Idem*, p. 393;
[318] Vide artigo 19.º n.º 1 alínea b) da Lei do Cibercrime: "*Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, 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.*".

Encobertas, quer ao magistrado do Ministério Público, quer ao Juiz de Instrução Criminal, consoante exista já inquérito ou não. Ora, salvo o devido respeito pela opinião contrária, não podemos concordar com o entendimento perfilhado, em virtude de entendermos que a referida autorização deve partir sempre do Juiz de Instrução Criminal, seja quando já existe um inquérito, seja quando ainda se esteja no âmbito da prevenção criminal.

Conforme já *supra* aludido, as ações encobertas em ambiente digital, enquanto método oculto de obtenção de prova, neutralizam e restringem alguns dos direitos fundamentais dos cidadãos alvo das mesmas, nomeadamente o direito à intimidade ou reserva da vida privada, à autodeterminação informacional ou informativa, à confidencialidade e integridade dos sistemas informacionais e à inviolabilidade do domicílio informático. Para garantir que é respeitado o princípio da proporcionalidade vindo de referir, com o recurso a um método tão restritivo de direitos fundamentais, o papel do Juiz de Instrução Criminal, enquanto juiz das garantias e liberdades, é absolutamente essencial. Como realça Anabela Rodrigues, "*Identifica-se inequivocamente um 'núcleo transnacional' na função do juiz, de garante das liberdades, presente em todas as fases do processo mas que sobressai nas fases que antecedem o julgamento – e na fase de investigação que é o inquérito – já que aqui são suscetíveis de se verificar os ataques mais graves às liberdades das pessoas. O juiz, dotado de independência e imparcialidade que a Constituição e o seu estatuto lhe conferem, é o único sujeito processual que pode por isso, assumir plenamente o papel de garante dos direitos, liberdades e garantias dos cidadãos.*"[319].

A nosso ver, a garantia dos direitos fundamentais dos cidadãos visados por uma ação encoberta em ambiente digital não se satisfaz com a mera autorização por parte do magistrado do Ministério Público, ainda que depois seja submetida a validação do Juiz de Instrução Criminal. Por muito neutro que o digno magistrado deva ser, a verdade é que este nunca será uma pessoa totalmente desinteressada da investigação, bem pelo contrário. Ao passo que o Juiz de Instrução Criminal se encontra numa posição muito mais objetiva, posição esta que lhe fornece a capacidade de garantir o devido respeito pelos direitos liberdades e garantias dos indivíduos. Perfilhamos, nesta senda, a tese defendida por Fátima Mata-Mouros, de acordo com a qual "*Trata-se de evitar o irreparável. Evitar a verificação de prejuízos injustificados de direitos fundamentais. Ora, uma tal preocupação não pode ser confiada ao próprio responsável pela investigação que, por mais objetividades que coloque na sua apreciação, será sempre interessado no resultado da sua*

[319] RODRIGUES, Anabela, "A Jurisprudência Constitucional Portuguesa e a Reserva do Juiz nas Fases Anteriores ao Julgamento ou a Matriz Basicamente Acusatória do Processo Penal", In: DIAS, Jorge de Figueiredo, *et al.*, *XXV Anos de Jurisprudência Constitucional Portuguesa – Colóquio Comemorativo do XXV Aniversário do Tribunal Consti*tucional, Coimbra Editora, 2009, p. 49.

atividade, numa palavra, juiz em causa própria. Não é pelo facto de o procurador dever permanecer neutro que ele age necessariamente de maneira imparcial. E mesmo que uma tal crítica possa igualmente ser apontada ao juiz de instrução, a verdade é que aquele se encontra numa posição mais favorável do que o ministério público, para respeitar a objetividade do inquérito, uma vez que a este último incumbe o duplo papel de acusador e investigador."[320]. Assim, entendemos que a realização de uma ação encoberta em ambiente digital deve depender de uma autorização prévia, emitida em todas as situações pelo Juiz de Instrução Criminal e só por este.

O novo regime jurídico a criar deverá também debruçar-se sobre o procedimento a implementar relativamente à adoção de identidade fictícia por parte do agente encoberto. Como já tivemos oportunidade de evidenciar no presente estudo, uma das características do ambiente digital é a ausência de contacto pessoal e físico entre as pessoas que interagem entre si, sendo que o mesmo se aplica no seio das ações encobertas no referido ambiente, na relação estabelecida entre agente encoberto e visado. Um dos primeiros aspetos que entendemos que o novo diploma legal deve prever é a atribuição de identidade fictícia ao agente encoberto, seja este um órgão de polícia criminal ou um terceiro, ao contrário do que se encontra atualmente previsto na Lei n.º 101/2001. Ao terceiro também deve ser atribuída a oportunidade de não ter que revelar a sua verdadeira identidade e sim adotar uma nova, que até se pode revelar mais conveniente para a investigação criminal em curso.

Neste seguimento, entendemos que, caso seja no melhor interesse da investigação e essencial para o sucesso desta, deve ser possível a adoção de múltiplas identidades fictícias por um só agente encoberto – sendo certo, no entanto, que todas se devem encontrar devidamente autorizadas e aprovadas, quer pelo responsável da investigação, quer pelo Ministério da Justiça. Não deverá, assim, ser dada liberdade ao agente encoberto para adotar as identidades que bem entender, mas antes todas devem passar pelo referido crivo. O entendimento vindo de expor aplica-se, igualmente, à criação de perfis conexos ao perfil ou perfis principais do agente encoberto, com o intuito de atribuir uma maior credibilidade aos mesmos. No que se refere à utilização de perfis com a aparência de uma pessoa conhecida ou próxima do visado pela ação encoberta em ambiente digital, entendemos que tal apenas será possível depois de obtido o devido consentimento por parte da referida pessoa. Caso tal não seja possível, seja porque a pessoa não dá o seu consentimento, seja porque o próprio pedido de consentimento deitaria por terra toda a ação encoberta, julgamos ser de rejeitar tal utilização – um entendimento diferente poderia resultar

[320] MATA-MOUROS, Fátima, *Juiz das Liberdades – Desconstrução de um Mito do Processo Penal*, Almedina, 2011, p. 23.

não só numa violação do direito à imagem do indivíduo, como colocaria potencialmente em risco a sua segurança.

Por forma a acautelar as especificidades das ações encobertas em ambiente digital, o novo regime a criar deverá abordar também os requisitos necessários para uma determinada pessoa adotar a posição de agente encoberto, requisitos estes que dizem respeito, maioritariamente, à necessidade de existência de vastos conhecimentos técnicos e informáticos, que em momento algum se confundem com os conhecimentos possuídos por um qualquer utilizador frequente da *internet*. Para que possa desempenhar o papel de agente encoberto, a pessoa em apreço deverá apresentar conhecimentos devidamente creditados, mormente ao nível da ocultação de identidade online, criptografia, protocolos de comunicação, *firewall*, sistemas de deteção de intrusão, técnicas de recolha/obtenção de prova digital, entre outros.

Esta necessidade de o agente encoberto em ambiente digital possuir conhecimentos técnicos e informáticos avançados é uma *faca de dois gumes*, uma vez que pode determinar o sucesso da ação encoberta, mas poderá também levar a que o agente encoberto se aproprie indevidamente de bens alcançados por meio da mesma sem que os demais – leia-se os que não possuem tantos conhecimentos – se apercebam de tal situação. Quer queiramos, quer não, ser portador de conhecimentos informáticos que a maioria dos demais não tem traz ao agente encoberto uma maior liberdade, no sentido em que pode adotar comportamentos indevidos que vão passar despercebidos. Nesta senda, entendemos ser necessária uma maior supervisão por parte de quem lidera a investigação criminal, devendo o relatório do agente encoberto ser junto aos autos sempre, com a devida ressalva da sua identidade. Este relatório deverá descrever detalhadamente todas as diligências encetadas e qual o propósito das mesmas, para que seja possível aferir a conformidade dos procedimentos levados a cabo.

O novo regime jurídico deve, ainda, estipular diretrizes relativamente aos meios físicos e informáticos a utilizar, isto é, aos agentes encobertos deve ser assegurado todos os meios necessários ao correto desempenho da ação encoberta em ambiente digital, nomeadamente computador e ligação segura à *internet*. No nosso entendimento, o computador a utilizar deverá pertencer à entidade que pretender realizar a ação encoberta, nunca se recorrendo ao computador pessoal do agente encoberto, por óbvias questões de segurança. Na mesma senda, não deverá ser permitido a este último utilizar o computador adstrito à ação encoberta para fins pessoais, assegurando assim a inexistência de contaminação da cadeia de custódia da prova. É também necessário garantir que existe uma ligação segura à *internet*, que permita ao agente encoberto

manter a sua identidade fictícia, e que não é possível aceder aos dados pessoais do mesmo, através da empresa fornecedora dos serviços de *internet*. Tendo em conta que as ações encobertas realizadas no ambiente digital não dispõem de uma componente de contacto físico, coloca-se a questão de saber se é possível o agente encoberto atuar a partir do conforto de sua casa e não das instalações do órgão de polícia criminal. Ora, somos da opinião que uma tal situação só se poderia concretizar caso fosse possível garantir a integridade e segurança da rede e ligações à *internet* utilizadas.

Por fim, no que concerne à utilização de *chatbots* e, bem assim, de inteligência artificial no âmbito das ações encobertas em ambiente digital, entendemos que tais ferramentas podem ser muito valiosas para a investigação criminal, aumentando exponencialmente a eficácia das mesmas. Contudo, existe também aspetos negativos – tratando-se de um *software*, é inerente a existência de falhas que podem comprometer toda a investigação, tais como a não deteção de indícios de crime e até a própria denúncia de que se está perante uma ação encoberta. Assim, a ser possível o recurso à inteligência artificial, entendemos que o *software* a utilizar deverá ser previamente testado de forma intensiva e posteriormente creditado, para que se possa reduzir ao máximo quaisquer potenciais falhas.

Face ao *supra* exposto, impõe-se a criação de um novo regime jurídico que abarque todos os aspetos mencionados e que se dedique exclusivamente às ações encobertas em ambiente digital. Motivo pelo qual se apresenta o seguinte esboço:

Regime Jurídico das Ações Encobertas em Ambiente Digital

Artigo 1.º - Objeto

1. *A presente lei estabelece o regime das ações encobertas realizadas em ambiente digital para fins de prevenção e investigação criminal.*
2. *Consideram-se ações encobertas em ambiente digital aquelas que sejam desenvolvidas, através de dispositivos informáticos e online, por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária ou dos Serviços de Estrangeiros e Fronteiras, para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade.*

Artigo 2.º - Âmbito de aplicação

As ações encobertas em ambiente digital são admissíveis no âmbito da prevenção e repressão dos crimes previstos nas alíneas i) a m) do artigo 1.º do Código de Processo Penal e nos artigo 3.º a 8.º e 19.º n.º 1 alínea b) da Lei do Cibercrime.

Artigo 3.º - Requisitos

1. *As ações encobertas realizadas em ambiente digital devem ser adequadas aos fins de prevenção e repressão criminais identificados em concreto, necessárias à descoberta de material probatório, e proporcionais quer àquelas finalidades quer à gravidade do crime em investigação.*
2. *Ninguém pode ser obrigado a participar em ação encoberta.*
3. *O funcionário da investigação criminal ou terceiro selecionado para desempenhar o papel de agente encoberto deverá possuir conhecimentos técnicos e informáticos devidamente creditados, nomeadamente ao nível da ocultação de identidade online, criptografia, protocolos de comunicação, firewall, sistemas de deteção de intrusão, técnicas de recolha de prova digital, entre outros.*
4. *A realização de uma ação encoberta em ambiente digital depende sempre de prévia autorização do Juiz de Instrução Criminal, quer a mesma se realize no âmbito da prevenção ou da repressão criminal.*
5. *Se a ação encoberta em ambiente digital se realizar no âmbito da prevenção criminal, cabe ao magistrado do Ministério Público a proposta da mesma, junto do Departamento Central de Investigação e Ação Penal, sendo o juiz do Tribunal Central de Instrução Criminal o responsável pela respetiva autorização.*
6. *A entidade responsável por supervisionar a realização da ação encoberta fará o relato da intervenção do agente encoberto à autoridade judiciária competente no prazo máximo de quarenta e oito horas após o termo daquela.*

Artigo 4.º - Proteção de funcionário e terceiro

1. *A autoridade judiciária ordenará sempre a junção ao processo do relato a que se refere o n.º 5 do artigo 3.º.*
2. *Oficiosamente ou a requerimento da entidade responsável por supervisionar a realização da ação encoberta, a autoridade judiciária competente pode, mediante decisão*

fundamentada, autorizar que o agente encoberto que tenha atuado com identidade fictícia ao abrigo do artigo 5.º da presente lei preste depoimento sob esta identidade em processo relativo aos factos objeto da sua atuação.

3. *No caso de o juiz determinar, por indispensabilidade da prova, a comparência em audiência de julgamento do agente encoberto, observará sempre o disposto na segunda parte do n.º 1 do artigo 87.º do Código de Processo Penal, sendo igualmente aplicável o disposto na Lei n.º 93/99, de 14 de Julho.*
4. *No caso previsto no número anterior, se ao agente encoberto tiverem sido atribuídas múltiplas identidades nos termos do n.º 3 do artigo 5.º da presente lei, deverá o Ministério Público requerer que o depoimento prestado pelo agente encoberto decorra de acordo com o disposto no artigo 4.º da Lei n.º 93/99, de 14 de Julho, ou, em alternativa, deverá o mesmo decidir sob que identidade deverá o agente encoberto prestar o seu depoimento.*

Artigo 5.º - Identidade fictícia

1. *Para o efeito do n.º 2 do artigo 1.º, os funcionários da investigação criminal e os terceiros podem atuar sob identidade fictícia.*
2. *A identidade fictícia é atribuída por despacho do Ministro da Justiça, mediante proposta do órgão diretivo da entidade que supervisiona a realização da ação encoberta em ambiente digital.*
3. *Poderão ser atribuídas ao agente encoberto múltiplas identidades, quer seja para o perfil através do qual interage com o(s) visado(s) pela ação encoberta, quer seja para a criação de perfis conexos.*
4. *Apenas será permitida a utilização de perfis com a aparência de uma pessoa conhecida do(s) visado(s) pela ação encoberta, caso exista autorização por parte da mesma nesse sentido.*
5. *As identidades referidas nos números anteriores são válidas por um período de seis meses prorrogáveis por períodos de igual duração, ficando o funcionário de investigação criminal ou o terceiro a quem as mesmas forem atribuídas autorizado a, durante aquele período, atuar sob a identidade fictícia, quer no exercício da concreta investigação quer genericamente em todas as circunstâncias do tráfico jurídico e social.*
6. *O despacho que atribui as identidades fictícias é classificado de secreto e deve incluir a referência à verdadeira identidade do agente encoberto.*

7. *Compete à entidade supervisora da realização da ação encoberta gerir e promover a atualização das identidade fictícias outorgadas nos termos dos números anteriores.*

Artigo 6.º - Recursos físicos e informáticos

1. *Ao agente encoberto deverá ser atribuído, pela entidade supervisora da ação encoberta, um computador para a realização da mesma.*
2. *Não é permitido ao agente encoberto utilizar o seu computador pessoal para a realização da ação encoberta, nem utilizar o computador atribuído para efeitos pessoais.*
3. *Ao agente encoberto deverá ser disponibilizada uma ligação segura à internet, em que não seja possível obter, através da mesma, dados pessoais do agente.*
4. *No seguimento do disposto no número anterior, deverá a entidade que supervisiona a ação encoberta garantir que as empresas fornecedoras de serviços de internet não divulgam os dados em apreço.*
5. *É permitido ao agente encoberto realizar a ação encoberta a partir de outra localização que não as instalações do órgão de investigação criminal, desde que seja possível garantir a integridade e segurança da rede e ligações à internet utilizadas.*

Artigo 7.º - Isenção de Responsabilidade

1. *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.*
2. *Se for instaurado procedimento criminal por ato ou atos praticados ao abrigo do disposto na presente lei, a autoridade judiciária competente deve, logo que tenha conhecimento de tal facto, requerer informação ao Juiz de Instrução Criminal que emitiu a autorização a que se refere o n.º 4 do artigo 3.º.*

CONCLUSÃO

O processo penal, como qualquer outro processo judicial, tem como finalidade máxima a realização da justiça, que passará necessariamente pela descoberta da verdade e o restabelecimento da paz jurídica. Contudo, tal finalidade não se consubstancia num fim absoluto, na medida em que a busca pela verdade deve ser norteada pelo respeito total dos direitos fundamentais que assistem aos sujeitos processuais.

A descoberta da verdade no âmbito do processo penal, inerente ao ideal de realização da justiça, prende-se com a descoberta de uma verdade material, por oposição a uma verdade meramente formal. Pretende-se com o processo penal atingir uma verdade acerca da realidade de como determinados factos tiveram lugar, obtida sempre na senda do estrito respeito pelos direitos fundamentais dos cidadãos, e não uma verdade formal, inquinada por influências exercidas pelos variados sujeitos processuais. Em última análise, será esta descoberta da verdade material que irá legitimar a necessidade e sujeição a certa sanção penal, que tem como escopo proteger os bens jurídicos fundamentais e reintegrar o agente do crime na sociedade.

Para que seja possível conhecer a realidade dos factos relativos à prática de determinado crime e, bem assim, a verdade material, torna-se necessário levar a cabo uma investigação criminal, marcada pela intensa recolha de material probatório. O Código de Processo Penal distingue meios de prova de meios de obtenção de prova, nos seus artigos 128.º a 190.º, sendo que inseridas nestes últimos encontram-se as ações encobertas, previstas na Lei n.º 101/2001, de 24 de Junho.

Nas últimas décadas resultou patente o aumento exponencial do recurso a métodos ocultos de investigação, fruto do progresso tecnológico. Com os novos meios à sua disposição, os meliantes adquiriram novas capacidades que, em última análise, os tornaram extremamente eficientes na atividade de impossibilitar a deteção da prática de crimes. Face a este panorama, foi necessário recorrer a meios capazes de contornar essas mesmas capacidades, por forma a atingir-se uma maior eficácia da investigação criminal. Assim como o crime que, inicialmente, se operava no plano físico, passou a ter lugar no plano digital, também as ações encobertas tiveram que se adaptar a esta nova realidade e foi também necessário começar a realizar ações encobertas no ambiente digital.

Sucede que, o diploma legal regulador das ações encobertas, a Lei n.º 101/2001 de 24 de Junho, foi equacionado e desenhado num período temporal em que todas estas novas tecnologias e ferramentas ou ainda não tinham aparecido ou ainda se encontravam numa fase

muito embrionária. Desde então, muitas foram as mudanças a que assistimos na sociedade e na forma como os criminosos se comportam e procedem à prática de crimes. O aparecimento da Lei do Cibercrime, a Lei n.º 109/2009 de 15 de Setembro, veio colmatar várias falhas e acautelar muitas situações quando se estava perante a prática de crimes informáticos ou operados por recurso a meios tecnológicos. No que diz respeito à realização de ações encobertas em ambiente digital, este diploma legal veio, no seu artigo 19.º, remeter a sua regulamentação para o Regime Jurídico das Ações Encobertas e para outros diplomas legais, tais como as normas previstas no Código de Processo Penal relativas à interceção de comunicações, quando seja necessário recorrer a meios e dispositivos informáticos.

Da investigação realizada no âmbito do presente estudo foi possível concluir que o regime jurídico atualmente em vigor, resultante de uma conjugação entre o Regime Jurídico das Ações Encobertas, a Lei do Cibercrime e as disposições legais relativas à interceção de comunicações, não acautela suficientemente todas as especificidades das ações encobertas em ambiente digital. Questões como a adoção de múltiplas identidades pelo agente encoberto, em virtude de no seio da ação não ter que se expor física e pessoalmente; a necessidade de estabelecimentos de requisitos a nível de conhecimentos informáticos; a imperatividade de o relatório do agente encoberto ser sempre junto aos atos; a garantia de que são atribuídos ao agente encoberto todos os recursos físicos e informáticos necessários à realização da ação encoberta com sucesso e segurança, são, entre outras, totalmente desconsideradas pelos diplomas legais *supra* mencionados.

Esta desconsideração faz com que os direitos, liberdades e garantias dos cidadãos afetados por um meio oculto de obtenção de prova como as ações encobertas, que por si só já provoca restrições suficientes aos mesmos, não sejam devidamente acautelados.

No nosso entendimento, não se pode conceder que tal situação assim permaneça num Estado de Direito como o vigente no nosso ordenamento jurídico. É necessário e urgente a criação de um novo regime jurídico, desenhado especificamente para as ações encobertas em ambiente digital, abarcando todas as suas diferentes características. Tendo por base o Regime Jurídico das Ações Encobertas atualmente em vigor, com algumas alterações, mínimos nuns casos e substanciais noutros, cremos que chegamos ao que nos parece ser um esboço bastante completo do que deverá ser o regime jurídico a criar para as ações encobertas em ambiente digital.

BIBLIOGRAFIA

ABADINSKY, Howard, *Organized Crime*, 10th Edition, Wadsworth Cengage Learning, 2013, disponível em https://bit.ly/3r4XAnH, último acesso em 26-01-2022;

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3ª edição atualizada, Universidade Católica Editora, 2009;

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição atualizada, Lisboa, Universidade Católica Editora, 2011;

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição reimpressão, Lisboa, Universidade Católica Editora, 2018;

ALMEIDA, Ivo de, *A Prova Digital*, Librum Editora, 2018;

ANDRADE, Manuel da Costa, "*Métodos Ocultos de Investigação (plädoyer para uma teoria geral)*", In: Que futuro para o Direito Processual Penal?, Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português, (Coord. Mário Ferreira Monte, Maria Clara Calheiros, Fernando Conde Monteiro, Flávia Noversa Loureiro), Coimbra, Coimbra Editora, 2009, pp. 525-551;

ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, 1992;

ANTON, Luis Felipe Ruiz, El Agente Provocador en el Derecho Penal, Madrid, Editoriales de Derech Reunidas, 1982;

ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2016;

ASCENÇÃO, José de Oliveira, *Estudos sobre Direito da Internet e da Sociedade de Informação*, Almedina, 2001;

BELEZA, Teresa Pizarro, e ISASCA, Frederico, *Direito Processual Penal – Textos*, Associação Académica da Faculdade de Direito de Lisboa, 1991/1992;

BRENNER, Susan W., *Cybercrime and the Law – Challenges, Issues, and Outcomes*, Northeastern University Press, 2012;

BRENNER, Susan, "Law, Dissonance, and Remote Computer Searches", In: *North Carolina Journal of Law and Technology*, Vol. 14, Issue 1, Article 14, 2012, p. 43-92, disponível em https://bityli.com/nlSKV, último acesso em 10-01-2022;

CAMPOS, Juliana Filipa Sousa, *O Malware como Meio de Obtenção de Prova em Processo Penal – A Investigação Oculta em Ambiente Digital*, Almedina, 2021;

CANOTILHO, J. Gomes, *Direito Constitucional e Teoria da Constituição*, 7ª Edição, Coimbra, Almedina, 2003;

CANOTILHO, J. Gomes, e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume I, 4ª edição, Coimbra Editora, 2007;

CANOTILHO, J. Gomes, e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume II, 4ª edição, Coimbra Editora, 2010;

CARRAPIÇO, Helena, "O Crime Organizado e as Novas Tecnologias: Uma Faca de Dois Gumes", In: Nação e Defesa, n.º 111, 3.ª Série, 2005, pp. 175-192, disponível em https://bityli.com/RsrHY, último acesso em 04-08-2021;

CARRELL, Nathan E., "Spying on the Mob: United States V. Scarfo – A Constitutional Analysis", In: *Journal of Law, Technology & Policy*, Vol. 2002, pp. 193-214, disponível em https://bityli.com/swtA7, último acesso em 04-08-2021;

CARRIER, Brian D., SPAFFORD, Eugene H., *An Event-Based Digital Forensic Investigation Framework*, From the proceedings of The Digital Forensic Research Conference, DFRWS, Baltimore, 2004, disponível em https://bityli.com/05APo, último acesso em 17-08-2021;

CARRIER, Brian D., SPAFFORD, Eugene H., *Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence*, From the proceedings of The Digital Forensic Research Conference, DFRWS, New Orleans, 2005, disponível em https://bityli.com/mZZqF, último acesso em 17-08-2021;

CASEY, Eoghan, *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, 3ª edição, Elsevier Inc. All, 2011, disponível em https://bityli.com/r8m8h, último acesso em 12-08-2021;

CASTRO, Catarina Sarmento e, "40 anos de "Utilização da Informática" - o artigo 35.º da Constituição da República Portuguesa", *In*: *E-Pública – Revista Eletrónica de Direito Público*, Vol. 3, n.º 3, Dezembro de 2016, pp. 42-66, disponível em https://bityli.com/06SxB, último acesso em 24-08-2021;

CLOUGH, Jonathan, Principles of Cybercrime, Cambridge University Press, 2010;

CONCEIÇÃO, Ana Raquel, *Escutas Telefónicas – Regime Processual Penal*, Lisboa, Quid Iuris, 2009;

CONCEIÇÃO, Ana Raquel, "Presunção da Inocência", *In*: Paulo Pinto de Albuquerque (Org.), *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, Volume II, Lisboa, Universidade Católica Editora, 2019, pp. 1069-1099;

CORREIA, João Conde, "Prova digital: enquadramento legal", *In:* Centro de Estudos Judiciários (Org.), *Cibercriminalidade e Prova Digital*, *Ebook*, 2018, pp. 23-37, disponível em https://bityli.com/0ZskJ, último acesso em 11-08-2021;

DAVIES, Gemma, "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers", In: The Journal of Criminal Law, Vol. 84(5), 2020, pp. 407-426, disponível em https://bityli.com/bDPGg, último acesso em 14-02-2022;

DAY, Christopher, "Intrusion Prevention and Detection Systems", In: *Computer and Information Security Handbook*, 3ª edição, Elsevier, 2017, pp. 1011-1025, disponível em https://bityli.com/RI6SO, último acesso em 26-08-2021;

DE BEER, Richard, STANDER, Adrie, e VAN BELLE, Jean-Paul, "Anti-Forensic Tool Use and Their Impact on Digital Forensic Investigations: A South African Perspective", *In*: *The Proceedings of the International Conference in Information Security and Digital Forensics*, Thessaloniki, Greece, 2014, pp. 7-20, disponível em https://bityli.com/b6EtJ, último acesso em 19-08-2021;

DEPARTMENT OF JUSTICE, Online Investigative Principles for Federal Law Enforcement Agents, 1999, disponível em https://bityli.com/LhlWr último acesso em 16-02-2022;

DIAS, Jorge de Figueiredo, *Direito Processual Penal*, Volume I, Reimpressão, Coimbra, Coimbra Editora, 2004;

FERREIRA, Manuel Cavaleiro de, *Curso de Direito Processual Penal*, Volume I e II, Lisboa, 1955;

GASPAR, António Henriques, "As Ações Encobertas e o Processo Penal", *In*: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, pp. 43-53;

GASPAR, António Henriques, "Princípios do Processo Penal Português e a Convenção", *In*: *Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais*, Volume II, Lisboa, Universidade Católica Editora, 2019, pp. 1125-1141;

GARFINKEL, Simon, "Anti-Forensics: Techniques, Detection and Countermeasures", *In*: *The 2nd International Conference on i-Warfare and Security (ICIW)*, Naval Postgraduate School, Dudley Knox Library, 2007, pp. 77-84, disponível em https://bityli.com/ahBIz, último acesso em 18-08-2021;

GERCKE, Marco, *Understanding Cybercrime: A Guide for Developing Countries*, 2ª edição, International Telecommunication Union Cybercrime Legislation Resources, 2011, disponível em https://bityli.com/rWo0q, último acesso em 27-08-2021;

GERCKE, Marco, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, International Telecommunication Union, 2012, disponível em https://bityli.com/CugPR, último acesso em 04-08-2021;

GÓMEZ, Raúl Sánches, "El agente encubierto informático", *In*: *La Ley Penal*, n.ºº 118, Sección Estudios, Enero-Febrero, 2016, disponível em https://bityli.com/JCMrM, último acesso em 14-03-2022;

GONÇALVES, Fernando, e ALVES, Manuel João, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina, 2009;

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

GONÇALVES, Fernando, ALVES, Manuel João, e VALENTE, Manuel Monteiro Guedes, O Novo Regime Jurídico do Agente Infiltrado, Comentado e Anotado – Legislação Complementar, Almedina, 2001;

GONZALEZ-CASTELL, Adán Carrizo, "El Agente Infiltrado en España y Portugual – Estudo Comparado a la Luz de las Garantias y de los Principios Constitucionales", In: Centro de Investigação do ISCPSI (Org.), *Criminalidade Organizada e Criminalidade de Massa – Interferências e Ingerências Mútuas*, coordenação de Manuel Monteiro Guedes Valente, Almedina, 2009, pp. 185-219;

HARRIS, Ryan, "Arriving at an anti-forensics consensus: Examining how todefine and control the anti-forensics problem", In: Digital Investigation, 3S, 2006, pp. 44-49, disponível em https://bityli.com/XEv6M, último acesso em 18-08-2021;

HILL, Joshua B., e MARION, Nancy E., Introduction to Cybercrime – Computer Crimes, Laws and Policing in the 21st Century, PSI Textbook, 2016;

HOFFMANN-RIEM, Wolfgang, RIBEIRO, Pedro Henrique, "A Proteção de Direitos Fundamentais de Confidencialidade e da Integridade de Sistemas Próprios de Tecnologia da Informação", *In*: *Revista de Direito Civil Contemporâneo*, Vol. 23, Ano 7, pp. 329-365, disponível https://bityli.com/sy7T3, último acesso em 24-08-2021;

HOLT, Thomas J., BOSSLER, Adam M., e SEIGFRIED-SPELLAR, Kathryn C., *Cybercrime and Digital Forensics – An Introduction*, Routledge, 2015;

HOLT, Thomas J., e MARAS, Marie-Helen, *Cybercrime Risks and Responses – Eastern and Western Perspectives*, editado por SMITH, Russell G., CHEUNG, Ray Chak-Chung, e LAU, Laurie Yiu-Chung, Palgrave Macmillian, 2015;

IRIGOYEN, Carmen Lapuerta, "El cibercrimen y el agente encubierto on line", s/d, disponível em https://bityli.com/uuxJF, último acesso em 24-08-2021;

JESUS, Francisco Marcolino de, *Os Meios de Obtenção da Prova em Processo Penal*, Almedina, 2011;

KERR, Orin, "Digital Evidence and The New Criminal Procedure", In: *Columbia Law Review*, Vol. 105:279, pp. 279-318, disponível em https://bityli.com/ZSIFl, último acesso em 16-08-2021;

KOOPS, Bert-Jaap, "Police investigations in Internet open sources:Procedural-law issues", *In*: *Computer Law and Security Review*, n.º 29, 2013, pp. 654-665, disponível em https://bityli.com/3GRTL, último acesso em 18-08-2021;

LOUREIRO, Joaquim, *Agente Infiltrado? Agente Provocador! – Reflexões sobre o 1.º Acórdão do T.E.D. Homem – 9.Junho.1998. Condenação do Estado Português*, Almedina, 2007;

LOUREIRO, Nuno Miguel, "A Responsabilidade Penal do Agente Encoberto", *In Revista do Ministério Público*, Separata, n.º 142, Ano 36, 2015, pp. 79-120;

MAGRIÇO, Manuel Eduardo Aires, *A Exploração Sexual de Crianças no Ciberespaço – Aquisição e Valoração de Prova Forense de Natureza Digital*, Sinapis Editores, 2013;

MANSON, Stephen, SHELDON, Andrew, e DRIES, Hein, "Proof: the technical collection and examination of electronic evidence", In: MANSON, Stephen, e SENG, Daniel (Org.), *Electronic Evidence*, University of London Press, 2011, pp. 285-338, disponível em https://bityli.com/zmrnU, último acesso em 18-08-2021;

MARTINS, A. G. Lourenço, "Criminalidade Informática", In: Associação Portuguesa do Direito Intelectual (Org.), *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003, pp. 9-41;

MARTINS, A. G. Lourenço, MARQUES, J. A. Garcia, e DIAS, Pedro Simões, *Cyberlaw em Portugal – O Direito das Tecnologias da Informação e da Comunicação*, Centro Atlântico, 2004;

MARQUES, Garcia, e MARTINS Lourenço, *Direito da Informática*, 2ª edição refundida e atualizada, Almedina, 2006;

MATA, Federico Bueno de, "El Agente Encubierto en Internet: Mentiras Virtuales para Alcanzar la Justicia", s/d, disponível em https://bityli.com/vduXB, último acesso em 22-02-2022;

MATA-MOUROS, Fátima, *Juiz das Liberdades – Desconstrução de um Mito do Processo Penal*, Almedina, 2011;

MEIREIS, Manuel Augusto Alves, "Homens de Confiança. Será o Caminho?", In: *II Congresso de Processo Penal – Memórias*, coordenação de Manuel Monteiro Guedes Valente, revisão científica de Germano Marques da Silva e Anabela Miranda Rodrigues, Almedina, 2006, pp. 81-101;

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

MENDES, Paulo de Sousa, *Lições de Direito Processual Penal,* Almedina, 2013;

MENKE, Fabiano, "A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito Alemão", *In*: *RJLB*, Ano 5, n.º 1, 2019, pp. 781-809, disponível em https://bityli.com/pyW2s, último acesso em 24-08-2021;

MESQUITA, Paulo Dá, *A Prova do Crime e O Que Se Disse Antes do Julgamento: Estudo sobre a Prova no Processo Penal Português, à Luz do Sistema Norte-Americano*, Coimbra Editora, 2011;

MONTE, Mário Ferreira, e LOUREIRO, Flávia Noversa, *Direito Processual Penal – Roteiro de Aulas*, 2ª edição, AEDUM, 2014;

MOURÃO, Helena, "O Efeito-à-Distância das Proibições de Prova no Direito Processual Penal Português", *In: Revista Portuguesa de Ciência Criminal*, n.º 4, Ano 16, Outubro-Dezembro 2006, pp. 575-620;

NEVES, Rita Castanheira, *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e Respetivo Regime Jurídico do Correio Eletrónico Enquanto Meio de Obtenção de Prova*, Coimbra Editora, 2011;

NUNES, Duarte Rodrigues, "A Incongruência do Património no Confisco 'Alargado' de Vantagens Provenientes da Prática de Crimes", *In*: Centro de Estudos Judiciários (Org.), *Recuperação de Ativos*, 2021, pp. 13-37, disponível em https://bityli.com/CApLT, último acesso em 28-01-2022;

NUNES, Duarte Rodrigues, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, Gestlegal, 2018;

Ó CIARDHUÁIN, Séamus, "An Extended Model of Cybercrime Investigations", *In: International Journal of Digital Evidence*, Summer 2004, Volume 3, Issue 1, disponível em https://bityli.com/jlUxB, último acesso em 18-08-2021;

OHM, Paul, "The Investigative Dynamics of the Use of Malware by Law Enforcement", *In: William & Mary Bill of Rights Journal*, Vol. 26, 2017, pp. 304-334, disponível em https://bityli.com/k0xtc, último acesso em 24-08-2021;

ONETO, Isabel, *O Agente Infiltrado – Contributo para a Compreensão do Regime Jurídico das Ações Encobertas*, Coimbra Editora, 2005;

PEREA, Inmaculada López-Barajas, "Nuevas Tecnologías Aplicadas a la Investigación Penal: El Registro de Equipos Informáticos", *In: Revista de Internet, Derecho Y Política*, n.º 24, 2017, disponível em https://bityli.com/ENMbg, último acesso em 04-08-2021;

PEREIRA, Alexandre Libório Dias, "Big Data, E-Health e «Autodeterminação Informativa»: A Lei 67/98, a Jurisprudência e o Regulamento 2016/679 (GDPR), s/d, disponível em https://bityli.com/kemxz, último acesso em 24-08-2021;

PEREIRA, Rui, "O 'Agente Encoberto' na Ordem Jurídica Portuguesa", In: Centro de Estudos Judiciários (Org.), *Medidas de Combate à Criminalidade Organizada e Económico-Financeira*, Coimbra Editora, 2004, pp. 11-41;

PEREIRA, Sandra, "A Recolha de Prova por Agente Infiltrado", In: *Prova Criminal e Direito de Defesa – Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal*, coordenação de Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto, Almedina, 2010, pp. 137-159;

PINHEIRO, Alexandre Sousa, *Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Associação Académica da Faculdade de Direito de Lisboa, 2015;

PRAIA, João de Matos-Cruz, "Proibições de prova em processo penal: algumas particularidades no âmbito da prova por reconhecimento e da reconstituição do facto", in *Julgar Online*, Dezembro de 2019;

RAMALHO, David Silva, "A Investigação Criminal na Dark Web", *In: Revista de Concorrência e Regulação*, n.º 14/15, Ano IV, Abril-Setembro 2013, pp. 383-429, disponível em https://bityli.com/GZzD1, último acesso em 11-08-2021;

RAMALHO, DAVID, "O Uso de Malware como Meio de Obtenção de Prova em Processo Penal", In: Revista da Concorrência e Regulação, Ano IV, N.º 16, 2013, pp. 195-243, disponível em https://bityli.com/MSSCH, último acesso em 10-01-2022;

RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Reimpressão, Almedina, 2019;

RIEKKINEN, Juhana, "Evidence of Cybercrime and Coercive Measures in Finland", In: *Digital Evidence and Electronic Signature Law Review*, n.º 13, 2016, pp. 49-66, disponível em https://bityli.com/m0J3G, último acesso em 04-08-2021;

RODRIGUES, Anabela, "A Jurisprudência Constitucional Portuguesa e a Reserva do Juiz nas Fases Anteriores ao Julgamento ou a Matriz Basicamente Acusatória do Processo Penal", *In*: DIAS, Jorge de Figueiredo, *et al.*, *XXV Anos de Jurisprudência Constitucional Portuguesa – Colóquio Comemorativo do XXV Aniversário do Tribunal Constitucional*, Coimbra Editora, 2009, pp. 47-65;

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente... A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1ª edição, Rei dos Livros, 2010;

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade Informática*, 1ª edição, Rei dos Livros, 2011;

SAMMONS, John, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, Syngress, 2012, disponível em https://bityli.com/t308C, último acesso em 19-08-2021;

SANTOS, Cristina Máximo dos, "As Novas Tecnologias da Informação e o Sigilo das Telecomunicações", In: *Revista do Ministério Público*, n.º 99, Ano 25, Jul/Set 2004, pp. 89-116, disponível em https://bityli.com/M6tnJ, último acesso em 04-08-2021;

SANTOS, Manuel Simas, SANTOS, João Simas, e LEAL-HENRIQUES, Manuel, *Noções de Processo Penal*, 2ª Edição, Lisboa, Rei dos Livros, 2011;

SANTOS, Paulo, BESSA, Ricardo, e PIMENTEL, Carlos, *Cyberwar – O Fenómeno, as Tecnologias e os Atores*, FCA, 2008;

SCHWABE, Jürgen, *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, MARTINS, Leonardo (Org.), Montevideo, 2005, disponível em https://bityli.com/SolcN, último acesso em 24-08-2021;

SHIPLEY, Todd G., BOWKER, Art, *Investigating Internet Crimes – An Introduction to Solving Crimes in Cyberspace*, Elsevier, 2014;

SIEBER, Ulrich, "Legal Aspects of Computer-Related Crime inthe Information Society – COMCRIME-Study", s/d, disponível em https://bityli.com/ZzVtW, último acesso em 04-08-2021;

SILVA, Flávio Manuel Carneiro da, "Apreensão e utilização processual de meios de prova existentes em material informático", In: Centro de Estudos Judiciários (Org.), *Meios de Obtenção*

de Prova e Medidas Cautelares e de Polícia, *Ebook*, 2019, pp. 13-39, disponível em https://bityli.com/q59Fx, último acesso em 11-08-2021;

SILVA, Germano Marques da, "Bufos, Infiltrados, Provocadores e Arrependidos – Os Princípios Democráticos e da Lealdade em Processo Penal", In: BELEZA, Teresa Pizarro (Org.), *Apontamentos de Direito Processual Penal*, III Vol., Lisboa, Associação Académica da Faculdade de Direito de Lisboa, 1995, pp. 61-69;

SILVA, Germano Marques da, *Curso de Processo Penal*, I, 4ª edição, Editorial Verbo, 2000;

SILVA, Germano Marques da, *Curso de Processo Penal*, II, 4ª edição, Editorial Verbo, 2008;

SILVA, Germano Marques da, *Introdução ao Estudo do Direito*, 5ª edição, Universidade Católica Editora, 2015;

SILVEIRA, Jorge Noronha e*, O Conceito de Indícios Suficientes no Processo Penal Português*, in Separata da Obra "Jornadas de Direito Processual Penal e Direitos Fundamentais", Coimbra, Almedina, 2004;

SINROD, Eric J., e REILLY, William P., "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", *In*: *Santa Clara High Tech Law Journal*, Vol. 16, Issue 2, Article 1, 2000, pp. 178-229, disponível em https://bityli.com/z7w8u, último acesso em 26-08-2021;

SOLOMON, Michael G., BARRETT, Diana, e BROOM, Neil, *Computer Forensics JumpStart*, Sybex, 2005;

SOUSA, Susana Aires de, "Agent Provocateur e Meios Enganosos de Prova. Algumas Reflexões", In: ANDRADE, Manuel da Costa, COSTA, José de Faria, RODRIGUES, Anabela Miranda, e ANTUNES, Maria João (Org.), *Liber Discipulorum para Jorge de Figueiredo Dias*, Coimbra Editora, 2003, pp. 1207-1235;

TARUFFO, Michele, *La Prueba, Artículos y Conferencias*, Monografias Jurídicas Universitas, Editorial Metropolitana;

TEIXEIRA, António Manuel de Jesus, Os Limites do Efeito-à-Distância nas Proibições de Prova no Processo Penal Português, 2013, Dissertação de Mestrado, Universidade Católica Portuguesa de Lisboa;

TEMPERINI, Marcelo, "Delitos Informáticos Y Cibercrimen: Técnicas Y Tendencias de Investigación Penal Y su Afectación a Los Derechos Constitucionales", s/d, disponível em https://bityli.com/sTzN5, último acesso em 04-08-2021;

TEMPERINI, Marcelo, e MACEDO, Maximiliano, "Nuevas herramientas de investigación penal: el agente encubierto digital", s/d, disponível em https://bityli.com/HI9kt, último acesso em 24-08-2021;

VACCA, John R., *Computer and Information Security Handbook*, 3ª edição, Elsevier, 2017, disponível em https://bityli.com/RI6SO, último acesso em 26-08-2021;

VACCA, John R., *Computer Forensics – Computer Crime Scene Investigation*, 2ª edição, Charles River Media, Inc., 2005, disponível em https://bityli.com/eX0io, último acesso em 16-08-2021;

VACIAGO, Giuseppe, "Remote Forensics and Cloud Computing: Na Italian and European Legal Overview", *In*: *Digital Evidence and Electronic Signature Law Review*, Vol. 8, 2011, pp. 124-129, disponível em https://bityli.com/C1hDq, último acesso em 24-08-2021;

VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova*, Almedina, 2019;

VALENTE, Manuel Monteiro Guedes, "A Investigação do Crime Organizado – Buscas Domiciliárias Noturnas, O Agente Infiltrado e Intervenção nas Comunicações", In: Centro de Investigação do ISCPSI (Org.), *Criminalidade Organizada e Criminalidade de Massa – Interferências e Ingerências Mútuas*, coordenação de Manuel Monteiro Guedes Valente, Almedina, 2009, pp. 159-184;

VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, 2001;

VERDELHO, Pedro, BRAVO, Rogério, e ROCHA, Manuel Lopes, *Leis do Cibercrime*, Vol. I, Centro Atlântico, 2003;

VERDELHO, Pedro, "A Obtenção de Prova no Ambiente Digital", In: *Revista do Ministério Público*, n.º 99, Ano 25, Jul/Set 2004, pp. 89-116, disponível em https://bityli.com/M6tnJ, último acesso em 11-08-2021;

VERDELHO, Pedro, "Cibercrime", In: Associação Portuguesa do Direito Intelectual (Org.), *Direito da Sociedade da Informação*, Vol. IV, Coimbra Editora, 2003, pp. 347-383;

WOO, Christopher, SO, Miranda, "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance", In: *Harvard Journal of Law & Technology*, Volume 15, Number 2, Spring 2002, pp. 521-538, disponível em https://bityli.com/JYLHG, último acesso em 10-01-2022;

JURISPRUDÊNCIA

Acórdão do Supremo Tribunal de Justiça, datado de 13 de Janeiro, relativo ao processo n.º 98P999, disponível em https://bityli.com/FHKjC, último acesso em 26-07-2021;

Acórdão do Supremo Tribunal de Justiça, datado de 09 de Fevereiro, relativo ao processo n.º 1/09.3FAHRT.L1.S1, disponível em https://bityli.com/OYgK9, último acesso em 15-03-2022;

Acórdão do Supremo Tribunal de Justiça, datado de 14 de Março, relativo ao processo n.º 07P21, disponível em https://bityli.com/NJOyC, último acesso em 15-03-2022;

Acórdão do Supremo Tribunal de Justiça, datado de 31 de Março, relativo ao processo n.º 257/10.9YRCBR.S1, disponível em https://bityli.com/xWJBG, último acesso em 21-03-2022;

Acórdão do Supremo Tribunal de Justiça, datado de 11 de Julho, relativo ao processo n.º 1611/07, disponível em https://bityli.com/jwt9J, último acesso em 15-03-2022;

Acórdão do Supremo Tribunal de Justiça dos Estados Unidos da América, datado de 19 de Junho, relativo ao processo *Mapp v. Ohio*, disponível em https://bityli.com/YoEMM, último acesso em 15-03-2022;

Acórdão do Tribunal da Relação de Coimbra, datado de 21 de Novembro, relativo ao processo n.º 926/2001, disponível em https://bityli.com/aW1hl, último acesso em 15-03-2022;

Acórdão do Tribunal da Relação de Évora, datado de 30 de Janeiro, relativo ao processo n.º 2457/06-1, disponível em https://bityli.com/FBoYk, último acesso em 15-03-2022;

Acórdão do Tribunal da Relação de Évora, datado de 04 e Fevereiro, relativo ao processo n.º 196/08.3JAFAR.E1, disponível em https://bityli.com/VPeoU, último acesso em 27-07-2021;

Acórdão do Tribunal da Relação do Porto, datado de 08 de Janeiro, relativo ao processo n.º 1170/09.8JAPRT.P2, disponível em https://bityli.com/PpIYv, último acesso em 25-08-2021;

Acórdão do Tribunal Constitucional, datado de 24 de Março, relativo ao processo n.º 39/04, disponível em https://bityli.com/9pOOT, último acesso em 15-03-2022;

Acórdão do Tribunal Constitucional, datado de 28 de Março, relativo ao processo n.º 778/00, disponível em https://bityli.com/SoNwt, último acesso em 15-03-2022;

Acórdão do Tribunal Constitucional, datado de 18 de Maio, relativo ao processo n.º 93/88, disponível em https://bityli.com/twkVP, último acesso em 15-03-2022;

Acórdão do Tribunal Constitucional, datado de 14 de Agosto, relativo ao processo n.º 815/07, disponível em https://bityli.com/Kiu9n, último acesso em 21-08-2021;

Acórdão do Tribunal Constitucional, datado de 27 de Agosto, relativo ao processo n.º 773/15, disponível em https://bityli.com/jHMea, último acesso em 24-08-2021;

Acórdão do Tribunal Constitucional, datado de 14 de Outubro, relativo ao processo n.º 835/98, disponível em https://bityli.com/nXZaI, último acesso em 27-07-2021;

Acórdão do Tribunal Constitucional, datado de 5 de Dezembro, relativo ao processo n.º 594/03, disponível em https://bityli.com/f4jSI, último acesso em 14-03-2022;

Acórdão do Tribunal Europeu dos Direitos do Homem, datado de 23 de Dezembro , relativo ao processo n.º 27785/10, disponível em https://bityli.com/9Kvql, último acesso em 17-08-2021.