1

O AGENTE INFILTRADO *ONLINE* NO DIREITO PORTUGUÊS[1]

Duarte Rodrigues Nunes[2]

RESUMO

O legislador português transpôs a Convenção sobre o Cibercrime do Conselho da Europa para a ordem jurídica portuguesa através da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), que inclui, nos artigos 12.º a 19.º, vários meios de obtenção de prova específicos para a obtenção de prova digital (os previstos na

[1] **Como citar este artigo científico.** NUNES, Duarte Rodrigues. O agente infiltrado *online* no direito português. In: **Revista Amagis Jurídica**, Ed. Associação dos Magistrados Mineiros, Belo Horizonte, v. 14, n. 1, p. 11-70, jan.-abr. 2022.

[2] Juiz de Direito. Professor Convidado da Universidade Europeia. Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa. Investigador integrado do Centro de Investigação de Direito Penal e Ciências Criminais e não integrado do Centro de Investigação Jurídica do Ciberespaço, ambos da Faculdade de Direito da Universidade de Lisboa. Conferencista. Autor de cinco monografias jurídicas: Os meios de obtenção de prova da Lei do Cibercrime (Gestlegal, Coimbra, 2018, reimpressão, 2021), Revistas e Buscas no Código de Processo Penal (Gestlegal, Coimbra, 2019); O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada (Dissertação de Doutoramento, Gestlegal, Coimbra, 2019), Os crimes previstos na Lei do Cibercrime (Gestlegal, Coimbra, 2020) e Curso de Direito Penal, Parte Geral, Tomo I (Gestlegal, Coimbra, 2021). Autor de mais de 20 artigos publicados em revistas jurídicas portuguesas e estrangeiras e contribuições em obras coletivas em matéria de Direito Penal e Processual Penal e Criminologia (em geral e também– e sobretudo – em matéria de criminalidade organizada, terrorismo, criminalidade económico-financeira, cibercrime e investigação criminal) e Direito Civil (Direito das Obrigações). Endereço eletrónico: *duarterodriguesnunes@hotmail.com*

Convenção de Budapeste e outros dois, embora a Lei n.º 109/2009 não esgote os meios de obtenção de prova relativos à prova digital: perícias e exames estão no Código de Processo Penal), sendo um desses meios de obtenção de prova as ações encobertas *online*. As ações encobertas *online*, cuja eficácia pode ser potenciada através da utilização de meios ou dispositivos informáticos, têm-se mostrado úteis na resposta ao jogo ilícito, ao tráfico de estupefacientes, à pornografia infantil e à pedofilia *online*, tráfico de armas e ao branqueamento de capitais. Nas investigações na *Dark Web*, a integração do agente infiltrado numa comunidade *online* e a sua interação com criminosos pertencentes a essa comunidade permitem neutralizar os obstáculos criados por via da utilização de técnicas antiforenses, descobrir a identidade e a localização dos autores dos crimes e recolher provas dos crimes através da persuasão dos próprios suspeitos a cederem tais informações. No presente artigo, analisa-se, igualmente, a admissibilidade das ações encobertas *online* e os limites dessa admissibilidade no Direito português.

Palavras-chave: Agente infiltrado *online*, Ações encobertas *online*, Cibercrime, Investigação criminal, Lei n.º 109/2009, de 15 de setembro, Convenção sobre o Cibercrime do Conselho da Europa.

ABSTRACT

The Convention on Cybercrime of the Council of Europe was transposed to the Portuguese legal order through Law Nº 109/2009, of September 15th (Cybercrime Law), which includes in articles 12 to 19 several specific means of obtaining evidence for obtaining digital evidence (those provided for in the Budapest Convention and two others, although Law N.º 109/2009 does not exhaust the means of obtaining evidence relating to digital evidence: Expert Evidence and Examinations are provided for in the Code of Criminal Procedure), being Online Undercover Operations one of such means of obtaining evidence. Online Undercover Operations, whose effectiveness can be enhanced through the use of computer means or devices, have proven to be useful in responding to Illegal Gambling, Drug Trafficking, Child Pornography and Online Pedophilia, Arms Trafficking and Money Laundering. In Dark Web investigations, the integration of the undercover agent in an online community and its interaction with criminals belonging to that community allows to neutralize the obstacles created through the use of anti-forensic techniques, discovering the identity and location of the perpetrators

of crimes and the collection of evidence of crimes through the persuasion of the suspects themselves to give such information. This article also analyzes the admissibility of online undercover operations and the limits of its admissibility under Portuguese law.

Keywords: Online Undercover Agent, Online Undercover Operations, Cybercrime, Criminal investigation, Law No. 109/2009, of September 15th, Convention on Cybercrime of the Council of Europe.

1 INTRODUÇÃO

A evolução das tecnologias da informação e das comunicações nas últimas décadas modificou de forma indelével o modo de relacionamento entre as pessoas. A Internet mudou radicalmente a vida de milhões de pessoas ao permitir o acesso, em questão de segundos, em qualquer parte do Mundo (desde que se possua uma ligação à Internet), a um manancial de informação armazenado em

servidores localizados em todo o Mundo, bem como – graças ao surgimento do correio eletrónico, das comunicações por VoIP e das mensagens instantâneas – a comunicação praticamente instantânea e gratuita entre pessoas que, muitas vezes, se encontram em locais que distam centenas ou milhares de quilómetros. Também as empresas tiveram de passar a centrar muita da sua atividade económica no Ciberespaço para, beneficiando da possibilidade de se dirigirem a um universo de consumidores muito mais vasto, aumentarem os seus lucros, sabendo que, não o fazendo, perderão competitividade face às empresas que apostam na presença no mundo virtual.

Do mesmo modo, surgiram as redes sociais, que permitem a troca de informações de cariz geral (*Facebook*) ou profissional (*LinkedIn*) e que também criaram uma enorme mutação na vida quotidiana das pessoas, potenciando a interação entre milhões de pessoas, que muitas vezes não se conhecem pessoalmente e vivem em locais que distam milhares de quilómetros entre si, mas possuem interesses, ideias, gostos e projetos em comum.

Contudo, esta evolução tecnológica trouxe igualmente aspetos negativos, pois as vantagens proporcionadas pelas novas tecnologias também podem ser aproveitadas – e são – para a prática de crimes[3].

De acordo com a ONU[4], o Cibercrime é uma forma de crime transnacional em evolução e uma realidade complexa, decorrendo essa complexidade do facto de ocorrer no território sem fronteiras do Ciberespaço e do crescente envolvimento de organizações criminosas e terroristas e de criminosos de colarinho branco (muitas vezes organizados)[5]. O que reclama a criação de uma resposta

[3] Como se enfatiza no Relatório Explicativo da Convenção sobre o Cibercrime.

[4] *Vide www.unodc.org/unodc/en/cybercrime/index.html.*

[5] O uso de meios informáticos é, de resto, uma vertente essencial para a prossecução da atividade criminosa e para o apagamento das provas do cometimento de crimes no âmbito da criminalidade organizada, do terrorismo e da criminalidade económico-financeira.

urgente, dinâmica e internacional.

Os meios informáticos poderão ser utilizados para a prática de crimes extremamente graves como o tráfico de droga, armas, seres humanos e órgãos ou espécies protegidas, homicídios, extorsões, abuso sexual de crianças (muitas vezes precedido de assédio), difusão de pornografia infantil, espionagem, destruição ou danificação de infraestruturas críticas (energia, transportes, telecomunicações, mecanismos de defesa nacional, hospitais, centrais elétricas ou nucleares e outros setores altamente dependentes da informática, etc.), branqueamento de capitais, burlas cometidas de forma massiva, etc., sendo particularmente elevado o número de crimes informáticos que são cometidos todos os anos, não se olvidando que os cibercriminosos têm utilizado a pandemia do SARS-Covid 19 e os seus efeitos para intensificarem – e de forma particularmente intensa – a prática de crimes informáticos e de crimes "comuns" cometidos com a utilização de meios informáticos (*v.g.*, as burlas cometidas na Internet).

A utilização dos meios informáticos deve-se a, entre outros fatores, permitir apagar as barreiras psicológicas que muitas vezes existem quando o criminoso tem de encarar a vítima, atingir um número elevado de pessoas em todo o Mundo e dificultar a identificação e a localização do criminoso e a recolha de provas. Na verdade, como referem Pinto Palacios e Pujol Capilla (2017, p. 189 e ss.), a cibercriminalidade caracteriza-se pelo anonimato, tecnologia de falsificação, extensão global e impunidade.

De acordo com o saber adquirido, o correio eletrónico[6],

[6] Definido, na al. b) do n.º 1 do art. 2.º da Lei n.º 41/2004, de 18 de agosto, na redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto, como "qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha".

as comunicações por VoIP[7] e as mensagens instantâneas[8] são amplamente utilizados pelos criminosos para preparar e executar crimes e para suprimir as provas do seu cometimento, usufruindo da rapidez, anonimato e volatilidade das comunicações informáticas.

Tal dificulta de sobremaneira a sua deteção e, quando sejam utilizadas medidas antiforenses[9], também a sua interceção e gravação. Tais meios de comunicação permitem suplantar a distância entre os criminosos comparticipantes (para comunicarem entre si ou para

[7] A voz sobre o protocolo Internet (*Voice over Internet Protocol* - VoIP) – de que são exemplos o *Skype,* o *Facebook,* o *Whatsapp* ou o *Viber* – é uma tecnologia que permite ao utilizador realizar chamadas telefónicas através de uma rede de dados como a Internet, convertendo um sinal de voz analógico num conjunto de sinais digitais sob a forma de pacotes com endereçamento IP, que podem ser enviados através de uma ligação à Internet (preferencialmente em banda larga).
A utilização de comunicações através de VoIP dificulta a sua interceção, pois, sendo os dados encriptados, tal obriga à sua interceção em momento prévio ao da sua encriptação, o que, por seu turno, requer a instalação sub-reptícia de *software* apropriado no sistema informático em causa por parte das autoridades ("vigilância nas fontes"). Deste modo, às dificuldades técnicas, somam-se as dificuldades jurídicas, dado que a admissibilidade da "vigilância nas fontes" ("*Quellenüberwachung*") é extremamente controversa na Doutrina e na Jurisprudência [cfr. NUNES, 2018, p. 156 (incluindo nota 292)].

[8] Este tipo de serviço – de que são exemplos o *Whatsapp*, o *Signal* ou o Telegram – difere-se do *e-mail*, pois as conversações ocorrem em tempo real. Geralmente, os participantes na comunicação veem cada linha de texto imediatamente após ter sido escrita, tornando esse serviço mais próximo do serviço telefónico do que do serviço postal. As conversas podem ser transmitidas de forma criptografada para aumentar a privacidade.
Dos vários serviços de mensagens instantâneas, cumpre referir o Telegram, que é massivamente utilizado pelos criminosos, pela proteção da privacidade acrescida que proporciona. O Telegram baseia-se num protocolo criptográfico único em que são convertidas todas as conversações. Para um nível superior de segurança e de privacidade existem ainda os "*Secret Chat*" que se podem criar com qualquer contacto – em que há encriptação *end-to-end*, nada ficando nos servidores do Telegram. Nos restantes serviços do Telegram, as mensagens, fotos, vídeos e ficheiros são encriptados antes de serem armazenados nos servidores do Telegram com uma chave que só o Telegram possui, ficando protegidos das autoridades.

[9] *V.g.,* encriptação das mensagens, esteganografia, utilização de *firewalls*, *Botnets*, VPN ou *proxies*, da *Dark Web* e de programas como o Tor, *Freenet*, I2P, GNUnet, *Retroshare* ou *SafetyGate Invisible* e de criptomoedas, etc.

cometerem crimes que, de outro modo, jamais conseguiriam cometer) e/ou entre os criminosos e as vítimas. E, ao permitirem enviar todo o tipo de anexos, poderão ser utilizados para difundir/instalar em sistemas informáticos alheios toda a espécie de *malware*[10]. Este, uma vez instalado, permitirá obter credenciais de acesso (ao *homebanking*, a cartões de débito ou crédito, ao *e-mail*, a redes sociais ou a *sites* de natureza reservada que requerem a introdução de uma *password*), copiar ou aceder a dados armazenados nesses sistemas (por exemplo, para exercer chantagem sobre a vítima ou para espionagem industrial) ou vigiar toda a atividade aí desenvolvida[11]. E também para abordar as vítimas para, posteriormente, as burlar (como sucedeu com as famosas "cartas da Nigéria" ou burlas 4-1-9[12]), assediar menores para posteriores abusos sexuais (*Child Grooming*), etc.

Daí a necessidade de as autoridades lançarem mão de meios investigatórios que permitam obter informações armazenadas em/acedidas a partir de sistemas informáticos, suportes informáticos autónomos (*v.g.,* discos rígidos externos, *pen drives*, cds e dvds), *clouds*, etc. ou transmitidas através de sistemas informáticos, bem como dados de tráfego de comunicações e dados de base e de localização dos sistemas informáticos.

Ciente de toda esta realidade e da necessidade de adequar a Lei processual penal à mesma, sob pena de ineficácia, o Conselho da Europa adotou a Convenção sobre o Cibercrime, aberta à assinatura em Budapeste em 23 de novembro de 2001 (CCiber)[13], que inclui,

[10] O *malware* é um programa informático que visa permitir a quem o utiliza infiltrar-se num sistema informático alheio, com o intuito de causar prejuízos ou de obter informações (confidenciais ou não), que, de outro modo, não poderia obter. O *malware* pode aparecer sob a forma de código executável, *scripts* de conteúdo ativo, etc.

[11] Cfr. RAMOS (2014; p. 24, 35 e 59), e GLENNY (2012, p. 11).

[12] Relativamente às "burlas 4-1-9", *vide*, entre outros, ALBANESE (2007, p. 224-225) e ABADINSKY (2007, p. 206).

[13] E assinada por Portugal nessa mesma data, aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, e ratificada pelo Decreto do Presidente da República n.º 91/2009, de 15 de setembro.

nos seus arts. 16.º a 21.º, diversos meios de obtenção de prova dirigidos à obtenção de prova digital.

O legislador português previu e regulou, pela primeira vez no ordenamento jurídico português, meios de obtenção de prova específicos para a aquisição de prova digital na Lei n.º 109/2009, de 15 de setembro[14], diploma em que transpôs a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e a Convenção sobre o Cibercrime do Conselho da Europa para o Direito português.

Embora a Convenção sobre o Cibercrime do Conselho da Europa tivesse sido aprovada em 23/11/2001 (e assinada por Portugal nessa mesma data) e entrado em vigor em 01/07/2004[15] e de ser inequívoca a insuficiência dos meios de obtenção de prova previstos no Código de Processo Penal para investigar eficazmente a criminalidade informática, só em 2009 é que legislador previu e regulou meios de obtenção de prova específicos para a aquisição de prova digital. Isto, apesar de o Código de Processo Penal (CPP)[16] ter sido alvo de uma profunda reforma em 2007 (Lei n.º 48/2007, de 29 de agosto).

Até então, utilizavam-se os meios de obtenção de prova previstos no Código de Processo Penal, como as buscas e as apreensões. No entanto, estes meios de obtenção de prova estavam delineados para incidirem sobre realidades corpóreas e não para realidades incorpóreas, como são os dados informáticos[17].

[14] Doravante referida como Lei n.º 109/2009. O texto da Lei n.º 109/2009 poderá ser encontrado no url *http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis*.

[15] A introdução, na ordem jurídica portuguesa, de meios de obtenção de prova específicos para a investigação do Cibercrime não dependia, nem da entrada em vigor da Convenção nem da sua transposição para o Direito português.

[16] O texto Código de Processo Penal poderá ser encontrado no url *http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis.*

[17] Definidos no art. 2.º, al. b), da Lei n.º 109/2009, como "qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função".

Diversamente do que sucedeu com a generalidade dos Estados que assinaram a Convenção sobre o Cibercrime, o legislador português optou por, em lugar de inserir a regulação desses meios de obtenção de prova no CPP ou noutra legislação avulsa preexistente, elaborar uma nova Lei, na qual regulou os meios de obtenção de prova específicos para investigar a criminalidade informática.

O elenco dos meios de obtenção de prova previstos na Lei n.º 109/2009 (cfr. arts. 12.º a 19.º) é mais abrangente do que o elenco da Convenção sobre o Cibercrime, pois inclui dois meios de obtenção de prova [apreensão de correio eletrónico e registos de comunicação de natureza semelhante (art. 17.º) e ações encobertas *online* (art. 19.º)] que não estão previstos na Convenção sobre o Cibercrime.

Porém, os meios de obtenção de prova que podem ser utilizados na investigação do cibercrime não se limitam aos meios previstos na Lei n.º 109/2009, dado que meios de prova e de obtenção de prova que são tendencialmente utilizáveis na investigação desta forma de criminalidade como as perícias e os exames estão previstos no CPP (cfr. arts. 151.º e ss. e 171.º e ss., respetivamente).

2 ÂMBITO DE APLICAÇÃO DAS NORMAS RELATIVAS AOS MEIOS DE OBTENÇÃO DE PROVA

Nos termos do art. 11.º da Lei n.º 109/2009, salvo no caso da interceção de comunicações e das ações encobertas (que só poderão ser utilizados na investigação dos crimes especificados no art. 18.º, n.º 1, e no art. 19.º, n.º 1, dessa Lei, respetivamente), os demais meios de obtenção de prova poderão ser utilizados na investigação de crimes previstos nessa Lei[18] e de quaisquer crimes cometidos por

[18] Crimes de falsidade informática, de dano relativo a programas ou outros dados informáticos, de sabotagem informática, de acesso ilegítimo, de interceção ilegítima e de reprodução ilegítima de programa protegido (sobre cada um destes crimes, incluindo a finalidade da sua criminalização, o bem jurídico protegido, a natureza do crime, os elementos objetivos e subjetivos do tipo, as circunstâncias

meio de um sistema informático[19] ou cuja investigação requeira a recolha de prova em suporte eletrónico.

E, no n.º 2 desse art. 11.º, o legislador determina que o disposto nos arts. 12.º a 19.º da Lei n.º 109/2009 não prejudica o regime da Lei n.º 32/2008, de 17 de julho (relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações)[20]. Trata-se de uma norma que levanta enormes dificuldades interpretativas, dado que não clarifica se o art. 9.º da Lei n.º 32/2008 (que regula a utilização, no processo penal, de dados previamente conservados[21]) foi, ou não, revogado pelos arts. 12.º a 19.º da Lei n.º 109/2009[22], sendo que aquela norma, que apenas se aplica a crimes graves, acaba por conter um regime de utilização de dados conservados mais restritivo do que os arts. 12.º a 19.º da Lei n.º 109/2009, que se aplicam a um elenco de crimes muito mais amplo.

---

modificativas agravantes, a exclusão da ilicitude e da culpa, a prescrição, a punição (incluindo as molduras penais e a punibilidade da tentativa), as relações de concurso com outros crime, etc., *vide* NUNES, 2020b).

[19] Definido no art. 2.º, al. a), da Lei n.º 109/2009, como "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção".

[20] Doravante referida como Lei n.º 32/2008. O texto da Lei n.º 32/2008 poderá ser encontrado no url *http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1264A0004&nid=1264&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo*.

[21] As categorias de dados que são objeto de conservação constam do art. 4.º da Lei n.º 32/2008.

[22] A este respeito, entende-se maioritariamente que o art. 9.º da Lei n.º 32/2008 não foi revogado pelos arts. 12.º a 19.º da Lei n.º 109/2009, sendo minoritária a opinião contrária (que subscrevemos). Acerca desta questão, *vide* NUNES (2019, p. 557 e ss., com indicações bibliográficas).

3 OS MEIOS DE OBTENÇÃO DE PROVA PREVISTOS NA LEI N.º 109/2009 PARA ALÉM DAS AÇÕES ENCOBERTAS *ON-LINE*

O primeiro meio de obtenção de prova regulado na Lei n.º 109/2009 (art. 12.º) é a preservação expedita de dados informáticos, que consiste em ordenar a quem tenha a disponibilidade ou o controlo de quaisquer dados informáticos específicos armazenados num sistema informático que adote as medidas necessárias para proteger esses dados de tudo o que possa alterar ou deteriorar a sua qualidade ou o seu estado atual, mantendo-os a salvo de toda e qualquer modificação, danificação ou eliminação, para não comprometer a produção de prova.

O destinatário da ordem de preservação deverá preservar de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual (cfr. art. 12.º, n.º 4, da Lei n.º 109/2009).

A ordem deverá ser dada pela autoridade judiciária[23] ou pelo

[23] Conjugando o art. 12.º, n.º 2, da Lei n.º 109/2009 com o art. 1.º, al. b), do CPP (que contém o conceito legal de "autoridade judiciária), a competência para emitir tal ordem é do Ministério Público na fase do inquérito, do Juiz de Instrução Criminal na fase da instrução e do Juiz na fase de julgamento. O processo penal português é constituído por quatro fases, duas obrigatórias e duas facultativas. A primeira fase é o inquérito, findo o qual, será proferida uma decisão, no sentido de submeter (acusação), ou não (arquivamento), o arguido a julgamento. Essa decisão poderá ser impugnada mediante um requerimento de abertura de instrução, iniciando-se assim uma fase facultativa (a fase de instrução), no final da qual será proferida nova decisão, no sentido de submeter (pronúncia), ou não (não pronúncia), o arguido a julgamento; o requerimento de abertura de instrução será apresentado pelo arguido nos casos em que tenha existido acusação ou pelo assistente (que, em regra, será a vítima do crime) quanto o processo tenha sido alvo de arquivamento. Caso o arguido tenha sido acusado e, havendo instrução, tenha sido pronunciado, abrir-se-á uma nova fase obrigatória (a fase de julgamento). E, finda a fase de julgamento, poderá ocorrer uma outra fase facultativa, que é a fase de recurso.

órgão de polícia criminal[24], mediante autorização da autoridade judiciária competente ou em casos de perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe um relatório no qual se mencionam, de forma resumida, as investigações levadas a cabo, os seus resultados, a descrição dos factos apurados e as provas recolhidas (cfr art. 12.º, n.º 2, da Lei n.º 109/2009, conjugado com o art. 253.º do CPP).

A preservação expedita de dados informáticos é determinada sempre que seja considerada necessária para a descoberta da verdade e/ou para a prova (cfr. art. 12.º, n.º 1, da Lei n.º 109/2009), relativamente a qualquer tipo de crime[25].

A ordem de preservação terá de discriminar (sob pena de nulidade), a natureza dos dados a preservar, a sua origem e destino (se forem conhecidos) e o período de tempo pelo qual deverão ser preservados, até um máximo de três meses (prorrogável até ao limite máximo de um ano) (cfr. art. 12.º, n.ºs 3 e 5, da Lei n.º 109/2009).

De acordo com os arts. 2.º, al. b), e 12.º, ambos da Lei n.º 109/2009, a ordem de preservação poderá incluir qualquer tipo de dados informáticos (cfr. VERDELHO, 2006, p. 270; RODRIGUES, 2010, p. 439).

O segundo meio de obtenção de prova previsto na Lei n.º 109/2009, mais concretamente no art. 13.º, é a revelação expedita de dados de tráfego[26], que consiste em o destinatário de uma ordem de

[24] No art. 1.º, al. c), do CPP define-se "órgãos de polícia criminal" como "todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer atos ordenados por uma autoridade judiciária ou determinados por este Código".

[25] Cfr. NUNES (2018, p. 41), MESQUITA (2010, p. 98), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*. Existe um acervo de Jurisprudência dos Tribunais de recurso [Tribunal Constitucional, Supremo Tribunal de Justiça, Supremo Tribunal Administrativo e Tribunais de 2.ª Instância: Tribunais da Relação – Lisboa, Porto, Coimbra, Évora e Guimarães – e Tribunais Centrais Administrativos – Norte (Porto) e Sul (Lisboa) –] e de Pareceres da Procuradoria-Geral da República em *www.dgsi.pt*.

[26] Definidos no art. 2.º, al. c), da Lei n.º 109/2009, como "os dados informáticos

preservação expedita de dados informáticos indicar à entidade que lhe deu a ordem de preservação, logo que saiba, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, a fim de permitir identificar estes e de, por via disso, também eles serem alvo de uma ordem de preservação expedita de dados informáticos, sendo acessória face à preservação expedita de dados, pois a sua finalidade é apenas garantir a eficácia da preservação expedita de dados (no mesmo sentido, NUNES, 2018, p. 52; RODRIGUES, 2010, p. 444).

A revelação expedita de dados de tráfego visa, desde logo, solucionar as dificuldades que se poderão colocar, em termos de eficácia da preservação expedita de dados informáticos para a investigação, por força de, pelo modo de funcionamento da rede, o IP definir o modo como os dados informáticos são enviados através da rede, atribuindo um endereço numérico a cada sistema informático que esteja ligado à Internet (o endereço de IP) e fragmentando, se necessário, os dados que irão ser transmitidos em pacotes de dados ou datagramas (em que se incluem os dados da comunicação e a origem e o destino da comunicação), podendo cada pacote de dados seguir um trajeto diverso dos demais (como tenderá a ocorrer) para maior celeridade na transmissão (cfr. NUNES, 2018, p. 54).

Um terceiro meio de obtenção de prova previsto na Lei n.º 109/2009 (mais concretamente no art. 14.º) é a injunção para apresentação ou concessão do acesso a dados, que corresponde às *Production Orders* do Direito anglo-saxónico e consiste em a autoridade judiciária ordenar a quem tenha a disponibilidade ou o controlo sobre dados informáticos específicos e determinados (salvo dados de tráfego e de conteúdo de comunicações) armazenados num dado sistema informático que os comunique ao processo ou permita

relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente".

o acesso ao sistema informático onde estão armazenados sempre que, no decurso do processo, a obtenção de tais dados se mostre necessária para a produção de prova (cfr. art. 14.º, n.º 1, da Lei n.º 109/2009).

Com base na injunção para apresentação ou concessão do acesso a dados também pode ser ordenado aos fornecedores de serviço que comuniquem ao processo ou permitam o acesso a dados relativos aos seus clientes ou assinantes que não sejam dados de tráfego nem de conteúdo e que sejam por eles detidos. E permitam determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço, bem como a identidade, a morada postal ou geográfica e o número de telefone do assinante, qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento disponíveis com base num contrato ou acordo de serviços ou qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou acordo de serviços (cfr. art. 14.º, n.º 4, da Lei n.º 109/2009).

A injunção para apresentação ou concessão do acesso a dados incide sobre dados informáticos (salvo dados de tráfego ou de conteúdo de comunicações) e a chave de acesso à encriptação dos dados em causa (cfr. RAMALHO, 2017, p. 170). A ordem de fornecimento dos dados ou de permissão de acesso terá de especificar quais os dados cujo fornecimento ou acesso se pretende (cfr. art. 14.º, n.º 2, da Lei n.º 109/2009), para que o acesso incida apenas sobre os dados relevantes para a investigação e não ocorra um acesso indiscriminado a todos e quaisquer dados (cfr. VERDELHO, 2003, p. 377).

Todavia, nos termos do art. 14.º, n.º 5, da Lei n.º 109/2009, a ordem de apresentação ou concessão do acesso a dados não poderá ser dirigida ao arguido nem ao suspeito que ainda não tenha sido constituído arguido (cfr. NUNES, 2018, p. 72-73; VERDELHO, 2006, p. 271), a fim de salvaguardar o direito à não autoincriminação (cfr. NEVES, 2011, p. 235).

A injunção para apresentação ou concessão do acesso a dados incide sobre dados informáticos que já foram recolhidos e arquivados pelos seus detentores, não incluindo a obtenção de dados informáticos em tempo real nem a conservação de futuros dados de tráfego nem o acesso em tempo real ao conteúdo das comunicações[27], que terão que ser obtidos por via interceção de comunicações prevista no art. 18.º da Lei n.º 109/2009[28].

O não acatamento, pelo destinatário, da injunção para apresentação ou concessão do acesso a dados fá-lo-á incorrer na prática de um crime de desobediência[29].

A injunção para apresentação ou concessão do acesso a dados de dados informáticos poderá ser utilizada na investigação de qualquer tipo de crime[30].

Relativamente ao sigilo profissional, nos termos do art. 14.º, n.º 6, da Lei n.º 109/2009, a ordem de apresentação ou concessão do acesso a dados não poderá ser dirigida relativamente a sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista. Apesar de se especificarem alguns casos de sigilo profissional, consideramos que a norma abrange todas as atividades sujeitas a sigilo profissional.

Assim, à primeira vista, parece que o recurso à injunção para apresentação ou concessão do acesso a dados não é admissível em tais casos. Contudo, prevê-se no n.º 7 desse art. 14.º a possibilidade de quebrar o sigilo profissional.

---

[27] Cfr. RODRIGUES (2008, p. 336), NUNES (2018, p. 60), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*.

[28] Cfr. NUNES (2018, p. 60); PINHO (2012, p. 78), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*.

[29] Cfr. arts. 14.º, n.ºs 1 e 3, da Lei n.º 109/2009, e 348.º, n.º 1, al. a), do Código Penal. O texto Código Penal poderá ser encontrado no url *http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis*.

[30] Cfr. NUNES (2108, p. 69); MESQUITA (2010, p. 98), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*.

Por isso, é possível dirigir uma ordem de apresentação ou de concessão do acesso a dados relativamente a dados armazenados em sistemas informáticos utilizados para o exercício de atividades sujeitas a sigilo profissional, desde que o sigilo profissional tenha sido quebrado, por autorização do Juiz ou, nos casos previstos na Lei, do Ministério Público[31].

Por fim, não é compreensível que o art. 14.º da Lei n.º 109/2009 não preveja qualquer procedimento tendente a esconjurar situações de perigo na demora como sucede nos arts. 12.º, n.º 2, 15.º, n.º 4, e 16.º, n.º 2 (cfr. NUNES, 2018, p. 83-84). Em primeiro lugar, as situações de perigo na demora também poderão surgir no âmbito da injunção para apresentação ou concessão do acesso a dados.

E, em segundo lugar, tal possibilidade está prevista quanto à pesquisa de dados informáticos e à apreensão de dados informáticos, não se compreendendo uma tal diferença, pois a injunção para apresentação ou concessão do acesso a dados não é mais lesiva para os direitos fundamentais do que a pesquisa de dados informáticos e a apreensão de dados informáticos (podendo até ser menos lesiva do que a pesquisa de dados informáticos).

O quarto meio de obtenção de prova previsto na Lei n.º 109/2009 (art. 15.º) é a pesquisa de dados informáticos, que é uma busca no sistema informático ou em parte dele (ou num suporte de armazenamento de dados independente), consistindo em, quando tal seja necessário para a descoberta da verdade ou para a prova, as autoridades acederem a um sistema informático, a fim de localizarem dados informáticos que aí estejam armazenados.

A pesquisa de dados informáticos poderá ser utilizada na investigação de qualquer tipo de crime[32], sendo autorizada pela

[31] Acerca desta questão, com maiores desenvolvimentos, NUNES (2018, p. 73 e ss., com indicações bibliográficas).

[32] Cfr. NUNES (2018, p. 95-96), MESQUITA (2010, p. 98), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*.

autoridade judiciária (que, sempre que possível, deverá presidir à diligência), tendo o despacho que a autoriza um prazo de validade máximo de 30 dias, sob pena de nulidade (cfr. art. 15.º, n.º 2, da Lei n.º 109/2009).

Nos termos do art. 15.º, n.º 3, da Lei n.º 109/2009, a pesquisa também poderá ser realizada pelo órgão de polícia criminal sem prévia autorização da autoridade judiciária em duas situações:

a) mediante o consentimento de quem tiver a disponibilidade ou controlo dos dados informáticos em causa (devendo o consentimento ficar, por qualquer forma, documentado); ou

b) em casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

Terá de ser apresentado, em ambas as situações, à autoridade judiciária, um relatório que contenha, de forma resumida, as investigações levadas a cabo, os seus resultados, a descrição dos factos apurados e as provas recolhidas e, na situação referida em b), a realização da pesquisa terá de ser comunicada no mais curto espaço de tempo possível à autoridade judiciária competente, para validação (cfr. art. 15.º, n.º 4, da Lei n.º 109/2009).

Se, no decurso da diligência, surgirem razões para crer que os dados procurados se encontram noutro sistema informático ou numa parte diferente do sistema pesquisado (o que inclui os casos em que os dados estão armazenados numa *cloud*), mas são legitimamente acessíveis a partir do sistema inicial, o n.º 5 do art. 15.º da Lei n.º 109/2009 permite que a pesquisa seja estendida ao outro sistema informático ou à outra parte do sistema pesquisado mediante autorização da autoridade judiciária competente.

Relativamente ao sigilo profissional, nos termos do art. 15.º, n.º 6, da Lei n.º 109/2009, as pesquisas informáticas em sistemas informáticos utilizados para o exercício de uma atividade sujeita a sigilo profissional[33] terão de ser autorizadas e presididas pelo Juiz (não podendo sê-lo pelo Ministério Público, mesmo em casos de *periculum in mora* – ainda que com ratificação *a posteriori* do Juiz –, o que pode comprometer seriamente a eficácia da investigação), devendo ser previamente avisado o presidente do conselho local da Ordem dos Advogados ou da Ordem dos Médicos, o presidente do conselho diretivo ou de gestão do estabelecimento de saúde em que o médico em causa exerce funções, o presidente do conselho regional da Ordem dos Solicitadores e dos Agentes de Execução, o presidente da organização sindical dos jornalistas com maior representatividade ou, nos demais casos, entidade equiparada, para que esteja presente ou se faça representar. E o profissional visado pela diligência também poderá estar presente.

O quinto meio de obtenção de prova previsto na Lei n.º 109/2009, mais concretamente, no art. 16.º, é a apreensão de dados informáticos, que consiste em as autoridades obterem, para o processo, dados informáticos que se encontrem num sistema informático ou num suporte autónomo que tenham sido alvos de uma pesquisa informática ou de outro acesso legítimo[34], bem como dos programas necessários para aceder a esses dados[35].

[33] Entendemos que, apesar de se afirmar, no art. 15.º, n.º 6, da Lei n.º 109/2009, que se aplica ao sigilo profissional de médico, advogado ou jornalista, tal regime deverá aplicar-se em todos os casos em que a pesquisa informática seja realizada num sistema informático utilizado para o exercício de uma atividade sujeita a sigilo profissional.

[34] A que poderemos subsumir a recolha dos dados informáticos por um especialista no local onde se encontra o sistema informático, uma busca no local onde se encontra o sistema informático, uma revista ou o acesso ao sistema informático ou ao suporte autónomo por via de uma injunção para apresentação ou concessão do acesso a dados (cfr. RAMALHO, 2017, p. 133-134).

[35] A impressão, pelas autoridades, daquilo que consta de uma página da Internet ou de um perfil de uma rede social constitui uma apreensão de dados informáticos

A apreensão de dados informáticos é autorizada pela autoridade judiciária, sempre que tal seja necessário para a descoberta da verdade material e/ou para a prova (cfr. art. 16.º, n.º 1, da Lei n.º 109/2009), podendo ser utilizada na investigação de qualquer tipo de crime[36].

Nos termos do art. 16.º, n.ºs 2 e 4, da Lei n.º 109/2009, a apreensão poderá ser realizada pelo órgão de polícia criminal no decurso de pesquisa informática legitimamente ordenada e executada nos termos do art. 15.º da Lei n.º 109/2009 ou quando haja urgência ou perigo na demora, devendo ser dado conhecimento, no prazo de 72 horas, à autoridade judiciária competente, para validação.

Dispõe o art. 16.º, n.º 3, da Lei n.º 109/2009, que, no caso de serem apreendidos dados informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos que possam pôr em causa a privacidade do respetivo titular ou de terceiro, esses dados ou documentos são, sob pena de nulidade, apresentados ao Juiz, que ponderará a sua junção aos autos, tendo em conta os interesses do caso concreto[37].

Nos termos do art. 16.º, n.ºs 5 e 6, da Lei n.º 109/2009, as apreensões de dados em sistemas informáticos utilizados para o exercício da advocacia e das atividades médica e bancária terão de ser autorizadas e presididas por Juiz, devendo ser previamente avisado o presidente do conselho local da Ordem dos Advogados ou da Ordem dos Médicos, o presidente do conselho diretivo ou de gestão do estabelecimento de saúde em que o médico em causa exerce funções, o presidente do conselho regional da Ordem dos Solicitadores e dos Agentes de Execução, o presidente da organização sindical

(cfr. Acórdãos do Tribunal da Relação do Porto de 13-04-2016 e 05-04-2017, *in www.dgsi.pt*).

[36] Cfr. NUNES (2018, p. 127), MESQUITA (2010, p. 98), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*.

[37] Acerca desta questão, com maiores desenvolvimentos, NUNES, 2018, p. 120 e ss. (com indicações bibliográficas).

dos jornalistas com maior representatividade ou, nos demais casos, entidade equiparada, para que esteja presente ou se faça representar. E o profissional visado pela diligência também poderá estar presente.

De acordo com o art. 16.º, n.º 7, da Lei n.º 109/2009, a apreensão de dados informáticos poderá ser executada mediante:

a) a apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura;

b) a realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) a preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) a eliminação não reversível ou bloqueio do acesso aos dados.

E, no n.º 8 do mesmo preceito, no caso de a apreensão consistir na realização de uma cópia dos dados em suporte autónomo, a cópia terá de ser efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos serão certificados por meio de assinatura digital.

A opção por uma das formas de execução da apreensão não é arbitrária, devendo as autoridades optarem por aquela que, sendo adequada a prosseguir as finalidades da investigação, seja menos lesiva para os direitos fundamentais das pessoas atingidas pela diligência (cfr. NUNES, 2018, p. 136-137).

O sexto meio de obtenção de prova previsto na Lei n.º 109/2009, mais concretamente, no art. 17.º, é a apreensão de

mensagens de correio eletrónico ou registos de comunicações de natureza semelhante. Este preceito regula as situações em que, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, sejam encontradas mensagens de correio eletrónico ou registos de comunicações de natureza semelhante[38], sujeitando a sua apreensão ao regime da apreensão de correspondência prevista no Código de Processo Penal (arts. 179.º e 252.º)[39].

A apreensão de mensagens de correio eletrónico ou de registos de comunicações de natureza semelhante é autorizada pelo Juiz sempre que essa apreensão seja de grande interesse para a descoberta da verdade ou para a prova (cfr. art. 17.º da Lei n.º 109/2009), podendo ser utilizada na investigação de qualquer tipo de crime[40]. Pela especificidade face à apreensão de correspondência, a autorização só poderá ser concedida *a posteriori* (cfr. NUNES, 2018, p. 153) e não será possível proceder à restituição do correio eletrónico apreendido que seja irrelevante, pelo que o disposto nos n.ºs 1 e 3 do art. 179.º do CPP terá de ser aplicado com as necessárias adaptações à apreensão de mensagens de correio eletrónico ou de registos de comunicações de natureza semelhante.

Em situações de *periculum in mora*, os órgãos de polícia criminal poderão utilizar a medida cautelar e de polícia prevista no art.

[38] *V.g.,* SMS, MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações via *Whatsapp, Viber, Skype, Facebook*, etc.

[39] Esta opção do legislador português (pois não consta da Convenção sobre o Cibercrime um regime similar para a apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, que, não se tratando de comunicações intercetadas em tempo real, são apreendidos como quaisquer outros dados informáticos) é alvo de forte crítica, entendendo-se que a apreensão deveria ser regulada pelo art. 16.º da Lei n.º 109/2009 (cujo n.º 3 constitui uma salvaguarda suficiente) e não pelo regime da apreensão de correspondência, entendimento que também acolhemos. Acerca desta questão, com maiores desenvolvimentos, NUNES, 2018, p. 141-146 (com indicações bibliográficas).

[40] Cfr. NUNES (2018, p. 147), MESQUITA (2010, p. 98), e Acórdãos do Tribunal da Relação de Évora de 06-01-2015 e 20-01-2015, *in www.dgsi.pt*.

252.º do CPP (cfr. ALBUQUERQUE, 2011, p. 510), embora apenas se coloque a possibilidade de aplicação da medida prevista no n.º 3, pois, por força da especificidade do correio eletrónico e de registos de comunicação de natureza semelhante, que não inclui realidades equiparáveis a encomendas, jamais será possível aplicar a medida prevista no n.º 2 à apreensão de correio eletrónico ou de registos de comunicação de natureza semelhante (cfr. NUNES, 2018, p. 154).

Por força da remissão do art. 17.º da Lei n.º 109/2009 para o regime da apreensão de correspondência, nos termos do art. 179.º, n.º 1, al. a), do CPP, apenas poderão ser apreendidas mensagens de correio eletrónico ou outras realidades análogas que tenham sido enviadas pelo arguido ou suspeito ou que lhe tenham sido dirigidas, mesmo que sob nome diverso ou através de pessoa diversa.

Relativamente ao sigilo profissional e começando pelo defensor do arguido ou suspeito, nos termos do art. 179.º, n.º 2, do CPP, só poderá haver apreensão ou outra forma de controlo da correspondência quando existam fundadas razões para crer que essa correspondência constitui objeto ou elemento de um crime.

Quanto aos demais casos de sigilo profissional, os arts. 17.º da Lei n.º 109/2009 e 179.º do CPP nada referem a este aspeto. Contudo, dado que estamos perante uma apreensão, vale aqui *mutatis mutandis* o que afirmámos em matéria de apreensão de dados informáticos à luz do art. 16.º da Lei n.º 109/2009.

O sétimo meio de obtenção de prova previsto na Lei n.º 109/2009 (art. 18.º), é a interceção de comunicações, que consiste na interceção[41] de comunicações informáticas, onde se inclui a obtenção de dados de conteúdo de comunicações em tempo real[42] (correio eletrónico, SMS, MMS, conversações no Messenger, comunicações

[41] Definida no art. 2.º, al. e), da Lei n.º 109/2009 como "o ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros".

[42] Cfr. MESQUITA (2010, p. 122), VENÂNCIO (2011, p. 119), e Acórdãos do Tribunal da Relação de Lisboa de 03-05-2016 e 07-03-2017, *in www.dgsi.pt*.

realizadas no âmbito de *newsgroups,* chats, videoconferências e Webconferências, etc. (cfr. ALBUQUERQUE, 2011, p. 542; VENÂNCIO, 2011, p. 119), e comunicações realizadas por VoIP[43]) e de dados de tráfego (seja em tempo real seja de dados conservados nos termos da Lei n.º 32/2008) (cfr. art. 18.º, n.º 3, da Lei n.º 109/2009).

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 Criminal. E mediante requerimento do Ministério Público (cfr. art. 18.º, n.º 1, da Lei n.º 109/2009), devendo ser fixado um período que não pode ser superior a três meses, embora podendo ser sucessivamente prorrogado ilimitadamente. Desde que continuem a verificar-se os pressupostos legais da interceção de comunicações. E que cada prorrogação não ultrapasse o prazo máximo de três meses (cfr. art. 187.º, n.º 6, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009).

Nos casos de *periculum in mora*, a autorização da interceção de comunicações poderá concedida pelo Juiz do lugar onde eventualmente puder ocorrer a conversação ou comunicação ou da sede da entidade competente para a investigação criminal (embora apenas quando esteja em causa a investigação de um dos crimes previstos nas várias alíneas do n.º 2 do art. 187.º do CPP) (cfr. art. 187.º, n.º 2, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009). Do mesmo modo, a autoridade de polícia criminal poderá requerer diretamente a realização de uma interceção de comunicações ao Juiz sem qualquer intermediação do Ministério Público (cfr. art. 269.º, n.ºs 1, al. e), e 2, conjugado com o art. 268.º, n.º 2, in fine, ambos do CPP).

[43] Cfr. NUNES, 2019, p. 572, e também em 2020a, p. 31 e ss., e VENÂNCIO (2011, 2011, p. 119); contra, ANDRADE, 2009a, p. 165; e RAMALHO, 2017, p. 339 e ss.

Porém, nos termos do art. 11.º, n.º 2, al. b), do CPP, compete ao Presidente do Supremo Tribunal de Justiça autorizar a interceção, gravação e transcrição de conversações ou comunicações em que intervenham o Presidente da República, o Presidente da Assembleia da República ou o Primeiro-Ministro. E determinar a respetiva destruição, o que inclui a interceção de comunicações nos termos do art. 18.º da Lei n.º 109/2009.

Nos termos do art. 18.º, n.º 1, da Lei n.º 109/2009, a interceção de comunicações apenas poderá ser utilizada na investigação de crimes previstos na Lei n.º 109/2009 (arts. 3.º a 8.º) ou de crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico. Desde que constem do elenco do art. 187.º, n.ºs 1 e 2, do CPP[44] e visar as comunicações do arguido ou de suspeito que

[44] Artigo 187.º

1 - A interceção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas 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, quanto a crimes:

a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos;
b) Relativos ao tráfico de estupefacientes;
c) De detenção de arma proibida e de tráfico de armas;
d) De contrabando;
e) De injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;
f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou
g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.

2 - A autorização a que alude o número anterior pode ser solicitada ao juiz dos lugares onde eventualmente se puder efetivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes:

a) Terrorismo, criminalidade violenta ou altamente organizada;
b) Sequestro, rapto e tomada de reféns;
c) Contra a identidade cultural e integridade pessoal, previstos no título iii do livro ii do Código Penal e previstos na Lei Penal Relativa às Violações do Direito Internacional Humanitário;

ainda não tenha sido constituído arguido, de pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido (intermediário) ou da vítima de crime (mediante o respetivo consentimento) (cfr. art. 187.º, n.º 4, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009).

As provas obtidas num processo através da interceção de comunicações apenas poderão ser utilizadas noutros processos (em curso ou a instaurar) se tiverem resultado de interceções de comunicações que tenham incidido em meio de comunicação utilizado pelo suspeito, arguido, intermediário ou pela vítima e apenas quando seja indispensável à prova de crime relativamente ao qual seja possível recorrer a este meio de obtenção de prova. Sem prejuízo de os elementos obtidos poderem ser utilizados como *notitia criminis* (permitindo a instauração de um novo processo ou a ampliação do objeto daquele processo) (cfr. art. 187.º, n.º 7, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009).

De acordo com o art. 187.º, n.º 5, do CPP (aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009), terão de existir razões fundadas para crer que as comunicações entre o arguido e o seu defensor constituem objeto ou elemento de crime, podendo as provas ser utilizadas contra o arguido e o defensor[45]. Embora a Lei apenas se refira às comunicações entre o arguido e o seu defensor, discute-se se a norma inclui também os demais casos de comunicações

d) Contra a segurança do Estado previstos no capítulo i do título v do livro ii do Código Penal;
e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262.º, 264.º, na parte em que remete para o artigo 262.º, e 267.º, na parte em que remete para os artigos 262.º e 264.º, do Código Penal;
f) Abrangidos por convenção sobre segurança da navegação aérea ou marítima.
[...].

[45] Cfr. LEITE (2004, p. 46); SUSANO, (2009, p. 39); NUNES, 2019, p. 637, e ALBUQUERQUE (2011, p. 527); contra (entendendo que as provas apenas poderão ser utilizadas contra o defensor, a fim de não prejudicar a defesa), CONCEIÇÃO (2009, p. 112), e ANDRADE (2005, p. 221).

em que intervenham pessoas sujeitas ao dever de guardar segredo profissional[46].

O órgão de polícia criminal que efetuar a interceção de comunicações terá de lavrar o competente auto e elaborar um relatório, no qual indica as passagens relevantes para a prova, descreve de modo sucinto o respetivo conteúdo. E explica o seu alcance para a descoberta da verdade (cfr. art. 188.º, n.º 1, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009).

Nos termos do art. 188.º, n.º 3 a 5, do CPP, o órgão de polícia criminal deverá, no prazo de 15 em 15 dias, contado desde o início da primeira interceção efetuada nos autos ou da anterior apresentação, levar ao conhecimento do Ministério Público os correspondentes suportes técnicos e os respetivos autos e relatórios (cfr. art. 188.º, n.º 3, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009). Seguidamente, o Ministério Público, no prazo máximo de quarenta e oito horas, deverá levá-los ao conhecimento do Juiz (cfr. art. 188.º, n.º 4, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009). O Juiz, para se inteirar do conteúdo das comunicações, poderá ser coadjuvado, quando entender conveniente, por órgão de polícia criminal. E nomear, se necessário, intérprete para proceder à tradução das comunicações (cfr. art. 188.º, n.º 5, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009), devendo determinar a destruição imediata dos suportes técnicos e relatórios que, sendo manifestamente estranhos ao objeto do processo[47], digam respeito a pessoas que não pudessem ser alvo interceção de comunicações,

[46] Entendem que o art. 187.º, n.º 5, do CPP não se aplica a tais casos, NUNES (2019, p. 639 e ss.), e LEITE (2004, p. 48).
Diversamente, a Doutrina maioritária considera que o art. 187.º, n.º 5, do CPP também se aplica nestes casos, cfr. ANDRADE (2005, p. 220); ALBUQUERQUE (2011, p. 527); SILVA (2008, p. 252), SUSANO (2009, p. 41), NEVES (2011, p. 295 e ss.), RODRIGUES (2008, p. 291 e ss.), CONCEIÇÃO (2009, p. 111) e VALENTE, (2008, p. 92).

[47] A "manifesta estranheza" deverá ser interpretada como absoluta e manifesta irrelevância para a boa decisão da causa (cfr. CUNHA, 2008, p. 218).

abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado ou cuja divulgação possa afetar gravemente direitos, liberdades e garantias (cfr. art. 188.º, n.º 6, do CPP, aplicável *ex vi* do art. 18.º, n.º 4, da Lei n.º 109/2009).

O último meio de obtenção de prova expressamente previsto na Lei n.º 109/2009, mais concretamente, no seu art. 19.º, são as ações encobertas *online* ou em ambiente-informático-digital, de que nos vamos ocupar no presente artigo. Trata-se de mais um exemplo de consagração, na Lei n.º 109/2009, de um meio de obtenção de prova não previsto na Convenção sobre o Cibercrime, situação que, nas várias ordens jurídicas que conhecemos, apenas tem paralelo (e apenas a partir de 2015) na ordem jurídica espanhola (cfr. art. 282 bis, n.º 6, da Ley de Enjuiciamiento Criminal).

Existe, ainda, um meio de obtenção de prova que não está expressamente previsto na Lei n.º 109/2009: a busca *online*, que consiste na "infiltração clandestina num sistema informático para observação da sua utilização e leitura dos dados nele armazenados" (ANDRADE, 2009a, p. 166), que é realizada *online*, com recurso a meios técnicos e através da instalação sub-reptícia, nesse sistema informático, de um programa informático do tipo "Cavalo de Troia" (cfr. ALBUQUERQUE, 2011, p. 502 e 541; ANDRADE, 2009a, p. 166), podendo consistir num único acesso ou ocorrer de forma contínua e prolongada no tempo.

Não possuindo a nossa ordem jurídica preceito que preveja expressamente este meio de obtenção de prova, não existe acordo na Doutrina quanto à sua admissibilidade[48] e, entre os defensores da

[48] ALBUQUERQUE (2011, p. 502 e 545); CORREIA (2014, p. 42 e ss.) (embora apenas no âmbito de uma ação encoberta em ambiente informático-digital), e NUNES (2019, p. 809 e ss.), e também NUNES (2020a, p. 40 e ss.), pronunciam-se pela admissibilidade, ao passo que RAMALHO (2013b, p. 227), e também em RAMALHO (2017, p. 346 e ss.), NEVES (2011, p. 196 e ss., 248 e 273), RODRIGUES (2010, p. 474-475), RAMOS (2014, p. 91), BRITO (2018, p. 97), FIDALGO (2020, p. 153 e ss.), CAMPOS (2021, p. 81 e ss.), e JESUS (2011, p. 196), pronunciam-se no sentido oposto.

admissibilidade, não existe acordo quanto à norma habilitante[49].

Consideramos que a busca *online* é admissível no Direito português, à luz do art. 15.º da Lei n.º 109/2009. Todavia, quando a busca *online* seja executada de forma contínua e prolongada no tempo (*Daten-Monitoring*), possuirá uma danosidade à da interceção de comunicações. Por isso, operando-se uma interpretação conforme à Constituição, ainda que esta forma de execução da busca *online* seja admissível à luz do art. 15.º da Lei n.º 109/2009, deverá ser-lhe aplicado o regime (mais restritivo) da interceção de comunicações prevista no art. 18.º da Lei n.º 109/2009[50].

RAMALHO (2013b, p. 227), e também em RAMALHO (2017, p. 346 e ss.), FIDALGO (2020, p. 154), e CAMPOS (2021, p. 96), entendem que o art. 19.º, n.º 2, da Lei n.º 109/2009 não observa as exigências de segurança jurídica, densificação e qualidade da lei restritiva de direitos fundamentais e é incompatível com os ditames do princípio da proporcionalidade quando permite o recurso à busca *online* (e o mesmo sucede quanto à ação encoberta em ambiente informático-digital) para investigar crimes de pequena gravidade e, por isso, é inconstitucional quando aplicado às buscas *online*.

[49] Ao passo que ALBUQUERQUE (2011, p. 502 e 545), considera que a norma habilitante é o art. 15.º da Lei n.º 109/2009 (sendo uma eventual inconstitucionalidade decorrente de a obtenção de dados íntimos ou privados ocorrer sem intervenção judicial afastada pelo art. 16.º, n.º 3, da mesma Lei, ao impor uma intervenção judicial, ainda que *a posteriori*, no caso de serem obtidos dados informáticos dessa natureza no decurso da pesquisa informática ou de outro acesso legítimo a um sistema informático), CORREIA (2014, p. 42 e ss.), entende que a norma habilitante é o art. 19.º, n.º 2, do Lei n.º 109/2009, que permite a utilização de meios e dispositivos informáticos no decurso de uma ação encoberta *online*. Pela nossa parte, concordamos com Paulo Pinto de Albuquerque (2011), embora com as especificidades que referiremos no texto e que sempre temos defendido noutras publicações.

[50] Acerca da nossa opinião, com maiores desenvolvimentos, *vide* NUNES (2019, p. 809 e ss.), e também em NUNES (2020a, p. 40 e ss.).

4 CONCEITO DE AÇÃO ENCOBERTA. A UTILIDADE DA AÇÃO ENCOBERTA *ONLINE*

O legislador define ação encoberta no art. 1.º, n.º 2, da Lei n.º 101/2001, de 25 de agosto[51], como "aquela(s) que seja(m) desenvolvida(s) por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária[52] para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade", existindo na nossa ordem jurídica dois tipos de ação encoberta: a "clássica" (que corresponde à infiltração de um polícia ou de uma pessoa não pertencente às forças de segurança mas que atue sob a direção destas, no *milieu* criminoso e que está regulada na Lei n.º 101/2001) e a realizada em ambiente informático-digital[53] (regulada no art. 19.º da Lei n.º 109/2009).

Tendo em conta o conceito de ação encoberta do art. 1.º, n.º 2, da Lei n.º 101/2001, sendo hoje possível criar programas informáticos que simulam pessoas reais sem que quem esteja a interagir com estas pessoas virtuais se aperceba de que não se trata de uma pessoa verdadeira[54], suscita-se a questão da admissibilidade

[51] O texto da Lei n.º 101/2001 poderá ser encontrado no url *http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis.*

[52] Ou do Serviço de Estrangeiros e Fronteiras (SEF), nos casos em que a competência para a investigação do crime em causa seja do SEF (cfr. ALBUQUERQUE, 2011, p. 681; e art. 188.º, n.º 2, da Lei n.º 23/2007, de 4 de julho).
O texto da Lei n.º 23/2007 poderá ser encontrado no url *http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=920&tabela=leis.*

[53] Na epígrafe do art. 19.º da Lei n.º 109/2009, o legislador apenas fala em "ações encobertas". Contudo, a Doutrina vem-se referindo a estas ações encobertas como "ações encobertas em ambiente informático-digital", a fim de as destrinçar das ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto.

[54] Veja-se, por exemplo, o caso real em que uma imagem virtual, tipo *robot*, simulando uma menina filipina de 11 anos de idade, atraiu diversos predadores sexuais, levando à identificação de vários abusadores em diversos países (Caso Sweetie). Nesta situação, uma ONG (*Terre des Hommes*), constatando que existiam na Internet inúmeros casos de turismo sexual de crianças (uma forma de prostituição que leva à exploração sexual de mais de dois milhões de crianças em todo o Mundo, em regra, crianças de parcos recursos económicos, que são

do uso de *Cybercops* (agentes policiais virtuais) em ações encobertas em ambiente informático-digital. Na nossa ótica, entendemos que nada na Lei portuguesa o impede (pelo que as provas obtidas são lícitas e utilizáveis) (contra, RAMOS, 2017, p. 194), sendo que o argumento de que o art. 1.º, n.º 2, da Lei n.º 101/2001 exige que as ações encobertas sejam realizadas por "funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária" (esgrimido por RAMOS, 2017, p. 194), ou seja, por pessoas físicas, reais e que, por isso, tal possibilidade está vedada, não colhe.

Em primeiro lugar, nas ações encobertas "clássicas", é óbvio que o agente infiltrado só poderá ser uma pessoa real, sendo absolutamente impossível que a utilização de um agente infiltrado "virtual" no mundo físico pudesse ter alguma utilidade investigativa, pelo que o disposto no art. 1.º, n.º 2, da Lei n.º 101/2001 não é uma imposição de que o agente infiltrado seja uma pessoa física.

Em segundo lugar, a Lei n.º 101/2001 aplica-se *mutatis mutandis* às ações encobertas em ambiente informático-digital.

Em terceiro lugar, o que o art. 1.º, n.º 2, da Lei n.º 101/2001 prevê é que as ações encobertas sejam realizadas por agentes policiais

incentivadas a despir-se perante *webcams* a troco de quantias monetárias ínfimas e a, posteriormente, realizarem encontros pessoais com pedófilos, que culminam com abusos sexuais), sendo as imagens de abusos gravadas e partilhadas, em grupos restritos na Internet, com maior incidência na *Dark Web*. Por isso, esta ONG criou uma imagem virtual de uma menina filipina de 11 anos de idade (por serem as Filipinas o país mais afetado), que esteve *online* em salas de conversação pública durante 10 semanas, permitindo à ONG identificar mais de 1.000 adultos, de 71 países, dispostos a pagar para visualizar atos sexuais da referida "menor" através de *webcam.* Após a obtenção da identificação dos IPs dos abusadores, a ONG entregou essas informações à Interpol para que procedesse a uma investigação criminal. Trata-se de uma conduta subsumível à figura do agente encoberto e não do agente infiltrado (não se tratando, por isso, de uma ação encoberta) e que é levada a cabo por particulares sem a direção das autoridades, razão pela qual jamais estaremos perante uma conduta subsumível ao conceito legal de ação encoberta do art. 1.º, n.º 2, da Lei n.º 101/2001 e, consequentemente, à aplicação do regime jurídico das ações encobertas.

ou particulares sob o controlo das autoridades e não por particulares agindo *motu proprium*, pelo que, desde que o *Cybercop* seja controlado pelas autoridades, diretamente ou mediante o controlo do particular que controla o *Cybercop* (*v.g.,* uma empresa que produza esses programas informáticos), não vemos em que medida a Lei não é observada.

Em quarto lugar, não se antolha que a utilização do *Cybercop* (que terá de ficar devidamente documentada para ulterior controlo da legalidade da obtenção das provas) constitua uma lesão mais intensa de direitos fundamentais do que no caso de o agente infiltrado ser uma pessoa física, sendo que a legalidade da prova e a ausência de provocação ao crime poderão ser perfeitamente controladas.

E, por último, nada impede que um particular, sem agir sob o controlo das autoridades, leve a cabo uma "ação encoberta" e que as provas obtidas sejam lícitas e utilizáveis, contanto que não tenham sido obtidas mediante a prática de um crime ou, no mínimo, de um ilícito-típico (por funcionamento do princípio da unidade da ordem jurídica) ou de um modo que configure uma "violação particularmente grave da dignidade humana", porquanto o art. 19.º da Lei n.º 109/2009 (tal como as demais normas que regulam os meios de obtenção de prova) apenas se aplica às autoridades e aos particulares que atuem sob a direção das autoridades (cfr. NUNES, 2019, p. 544 e ss. e 909 e ss.; RAMALHO, 2017, p. 301).

No entanto, no caso do *Cybercop*, que não ouve nem visiona o que se passa no sítio da Internet, *chat, newsgroup*, etc., limitando-se a registar o que aí se passa, estamos perante o uso de meios e dispositivos informáticos, pelo que haverá que observar o disposto no art. 19.º, n.º 2, da Lei n.º 109/2009[55].

[55] E o mesmo sucederá no caso de o agente infiltrado *online* ser uma pessoa física que, em vez de assistir "presencialmente" (sempre ou apenas durante alguns períodos) ao que se vai passando no sítio da Internet, *chat, newsgroup*, etc., coloca o seu sistema informático a registar as ocorrências, sendo que, desde que seja observado o disposto no art. 19.º, n.º 2, da Lei n.º 109/2009, a prova obtida é lícita e utilizável (daí discordarmos de RAMALHO, 2017, p. 296, quando afirma que essa prova será, "*por natureza, ilícita*").

As ações encobertas *online* têm-se mostrado úteis na resposta ao jogo ilícito, ao tráfico de estupefacientes, à pornografia infantil e à pedofilia *online* (cfr. RAMALHO, 2013a, p. 408), ao tráfico de armas e ao branqueamento de capitais. E, nas investigações na *Dark Web*, a sua utilização permite ultrapassar os obstáculos à descoberta da identidade e da localização dos autores do crime e das respetivas vítimas e à obtenção das provas necessárias para a investigação (neutralizando-se os obstáculos criados por via da utilização de técnicas antiforenses) através da persuasão dos próprios suspeitos a cederem elementos que permitam a sua identificação e outras informações relevantes para a investigação por via da integração do agente infiltrado numa comunidade *online* e da sua interação com criminosos pertencentes a essa comunidade (que, nas relações com os demais membros, poderão descurar as suas defesas e cometer erros que permitam a sua identificação e proporcionem meios de prova às autoridades) (assim, RAMALHO, 2013a, p. 408-409).

A eficácia da ação encoberta pode, ainda, ser potenciada com a utilização de meios ou dispositivos informáticos (*v.g.,* realizando uma busca *online*), o que é permitido pelo art. 19.º, n.º 2, da Lei n.º 109/2009.

Contudo, quando os *websites* não permitam a interação entre o agente infiltrado e os outros membros, este meio de obtenção de prova terá pouca utilidade (cfr. RAMALHO, 2013a, p. 409).

Por fim, cumpre referir que o êxito da ação encoberta em ambiente informático-digital depende de o agente possuir uma "pegada digital", ou seja, um histórico credível e sedimentado na Internet e que seja compatível com a personalidade que assumirá na ação encoberta (cfr. RAMOS, 2017, p. 77-78).

5 OS VÁRIOS "ATORES" DAS AÇÕES "ENCOBERTAS"

Ao nível das ações "encobertas", encontramos diversos tipos de "atores", os quais, apesar da sua proximidade, não se confundem.

E nem todos são subsumíveis ao regime legal de ação encoberta, que apenas inclui o agente infiltrado.

Começando pelo agente encoberto (*Nicht offen ermittelnde Polizeibeamte*), o agente encoberto é aquele que, sem revelar a sua identidade verdadeira ou qualidade e com a finalidade de obter provas para a incriminação do suspeito ou obter uma *notitia criminis*, frequenta os meios conotados com a prática de crimes, sendo que, naquela ocasião, poderia estar qualquer outra pessoa e as coisas aconteceriam da mesma forma (cfr. MEIREIS, 1999, p. 155; NUNES, 2019, p. 831). Embora sem ganhar a confiança do visado, o agente encoberto poderá ir um pouco além da mera frequência de tais locais, assumindo o papel de comprador simulado de droga ou de outra mercadoria ilícita (*Scheinkäufer*) ou de vítima potencial (mendigo, toxicodependente, comerciante, prostituta, motorista de táxi, idoso, etc.) para acionar o chamamento de outros agentes estrategicamente colocados, para que estes, intervindo imediatamente, detenham o criminoso em flagrante delito (cfr. ROXIN; SCHÜNEMANN, 2012, p. 306; NUNES, 2019, p. 831), podendo mesmo entabular conversa com os suspeitos que ali se encontrem (cfr. SOINÉ, 2010, p. 601; NUNES, 2019, p. 831-832).

No plano informático-digital, a conduta do agente encoberto pode consistir no "patrulhamento" de sítios da Internet, *chats* ou *newsgroups* abertos ou acedidos com o consentimento de um dos participantes[56], de redes *peer to peer* ou de outras "zonas de risco" do mundo virtual ou na criação de *websites* para identificar suspeitos da prática de um determinado crime (*v.g.,* em matéria de pornografia

[56] No caso do agente encoberto, o participante que consente/permite que o agente aceda a um sítio da Internet, *chat* ou *newsgroup* fechado terá de estar "conluiado" (*v.g.,* ser um informador da polícia) com o agente encoberto, conhecendo as finalidades do mesmo. Pelo contrário, se o agente tiver "usufruído" da confiança desse participante (que desconhece as finalidades do agente), estaremos perante um agente infiltrado, precisamente porque existiu um ganho de confiança, que caracteriza o agente infiltrado (no mesmo sentido, RAMALHO, 2017, p. 295).

infantil) (assim, NACK, 2008, p. 542)[57].

E continuamos perante um agente encoberto nos casos em que o agente participa em *chats, websites, blogs* ou fóruns livremente acessíveis (ainda que mediante registo prévio e a utilização de um *nickname*, em que não se distingue do *modus operandi* dos demais frequentadores), desde que não tome a iniciativa de interagir com os demais participantes e se limite a visionar os conteúdos que vão sendo partilhados[58].

A atuação do agente encoberto não está sujeita ao regime das ações encobertas da Lei n.º 101/2001 nem do art. 19.º da Lei n.º 109/2009, sendo um meio de obtenção de prova atípico admissível à luz do art. 125.º do CPP[59].

Por seu turno, o agente infiltrado (*Verdeckte Ermittler*, *Undercover agent*) é aquele que, sem revelar a sua identidade verdadeira e a sua qualidade, ganha a confiança pessoal do suspeito e infiltra-se no meio criminoso em causa (*v.g.,* numa organização criminosa), mantendo-se a par dos acontecimentos, acompanhando a execução dos factos e praticando atos preparatórios ou mesmo de execução (caso tal se mostre necessário, mas sem determinar quem quer que seja à prática de infrações), com a finalidade de obter provas para a incriminação do suspeito ou para obter uma *notitia criminis*, atuando de forma prolongada no tempo e, tratando-se de um elemento das autoridades policiais, atuando com uma identidade fictícia (cfr. NUNES, 2019, p. 832-833).

No plano informático-digital, a conduta do agente infiltrado consistirá em frequentar o mundo virtual utilizando uma identidade fictícia (*in casu*, bastará um *nickname*, não havendo que aplicar,

[57] Um exemplo disso é o Caso Sweetie a que fizemos referência.

[58] Neste sentido, embora em termos não totalmente coincidentes com o nosso entendimento, RAMALHO (2017, p. 297).

[59] Cfr. NUNES (2018, p. 201) e ss., e também em NUNES (2019, p. 838-839, com maiores desenvolvimentos e referências bibliográficas); contra, RAMALHO (2017, p. 289).

por desnecessidade, o regime do art. 5.º da Lei n.º 101/2001) (cfr. SOINÉ, 2014, p. 250; NUNES, 2019, p. 833, incluindo a nota 2.817), ganhando a confiança dos visados, mantendo-se a par dos acontecimentos e acompanhando a execução dos factos, interagindo com outros participantes em *chats, websites, blogs* ou fóruns (livremente acessíveis ou de acesso reservado) (cfr. RAMALHO, 2017, p. 295-296) e praticando atos preparatórios ou mesmo de execução (caso tal se mostre necessário, mas sem determinar ninguém à prática de infrações).

A atuação do agente infiltrado está sujeita ao regime das ações encobertas da Lei n.º 101/2001 e do art. 19.º da Lei n.º 109/2009 (cfr. NUNES, 2019, p. 838).

Por seu turno, o agente provocador (*Lockspitzel*, *agent provocateur*) é aquele que, embora sem querer o crime em si mesmo, mas pretendendo sujeitar o visado a um processo penal e, consequentemente, a uma pena, convence-o a cometer um crime que, não fosse a atuação do agente provocador, jamais cometeria (cfr. NUNES, 2019, p. 833)[60]. Ao nível da comparticipação criminosa, consoante o modo como atua, o agente provocador poderá assumir o papel de instigador ou mesmo de autor mediato (cfr. NUNES, 2019, p. 834).

No plano informático-digital, a conduta do agente provocador consiste em frequentar o mundo virtual, com utilização de uma identidade fictícia e convencer outra pessoa a cometer um crime que, se não fosse a conduta do agente, jamais cometeria (assim, NUNES, 2019, p. 834.).

[60] Contudo, para que se possa falar em provocação ao crime, não basta que o agente provocador atue sobre o provocado para o convencer a cometer o crime, sendo ainda necessária a existência de um nexo de causalidade entre a conduta do agente provocador e o facto praticado pelo provocado que permita concluir que, se não fosse a atuação daquele, este jamais teria praticado esse facto (cfr. ALBUQUERQUE, 2011, p. 682-683).

A conduta do agente provocador, pela violação das garantias fundamentais do processo penal que acarreta, constitui um método proibido de prova nos termos do art. 126.º, n.º 2, al. a), do CPP (cfr. ANDRADE, 1992, p. 231-232).

O "homem de confiança" (*V-Mann* ou *V-Person*) é uma pessoa não pertencente às instâncias formais de controlo (podendo mesmo pertencer ao *milieu* criminoso) que coopera com estas (sob a direção destas), assumindo uma conduta que, consoante a situação em concreto, configurará a atuação de um agente encoberto, infiltrado ou provocador (cfr. ELLBOGEN, 2004, p. 45; NUNES, 2019, p. 835). No plano informático-digital, a conduta do "homem de confiança" corresponderá à atuação do tipo de agente que "encarnar" (cfr. NUNES, 2019, p. 835).

A atuação do "homem de confiança" apenas estará sujeita ao regime das ações encobertas da Lei n.º 101/2001 e do art. 19.º da Lei n.º 109/2009 nos casos em que seja subsumível ao *modus operandi* do agente infiltrado, tal como definido supra.

A utilização de "homens de confiança" nas ações encobertas em ambiente informático-digital tenderá a ser muito menos necessária do que no caso das ações encobertas "clássicas", pois o agente policial não tem de agir "presencialmente" e pode ocultar a sua identidade utilizando *nicknames*. Todavia, o recurso aos "homens de confiança" em ações encobertas *online* poderá ser necessário em casos em que o êxito da ação encoberta requeira que o agente seja um particular integrado no *milieu* criminoso ou possua conhecimentos técnicos específicos sem os quais as autoridades não conseguiriam infiltrar-se em determinas áreas (*v.g.,* no caso de *hackers* contratados pelas autoridades para utilização dos seus especiais conhecimentos para fins legítimos) (no mesmo sentido, RAMALHO, 2017, p. 299), bem como em situações em que o agente tenha de ser alguém com uma "pegada digital" credível e consonante com a personalidade que terá de assumir na ação encoberta e nenhum agente policial possua uma tal "pegada" nem seja possível "construí-la" em tempo útil.

6 AS AÇÕES ENCOBERTAS NO DIREITO PORTUGUÊS

O regime geral das ações encobertas consta da Lei n.º 101/2001, na qual se consagra o conceito legal de ação encoberta (art. 1.º, n.º 2), o catálogo de crimes e demais requisitos materiais e procedimentais (arts. 2.º e 3.º), o regime da inquirição do agente infiltrado (art. 4.º), a possibilidade de utilização de identidade fictícia e o respetivo procedimento de atribuição (art. 5.º) e uma causa de exclusão da ilicitude da conduta do agente infiltrado (art. 6.º)[61]

Por seu turno, o art. 19.º da Lei n.º 109/2009 contém o regime específico das ações encobertas em ambiente informático digital, embora apenas quanto ao catálogo de crimes (n.º 1) e à possibilidade de utilizar cumulativamente meios e dispositivos informáticos (n.º 2), contendo uma remissão para o regime contido na Lei n.º 101/2001 no seu proémio.

7 REQUISITOS LEGAIS DAS AÇÕES ENCOBERTAS EM AMBIENTE INFORMÁTICO-DIGITAL

O regime jurídico das ações encobertas em ambiente informático-digital resulta do art. 19.º da Lei n.º 109/2009, conjugado com a Lei n.º 101/2001[62], aplicando-se aquele preceito às matérias nele reguladas e este diploma às matérias não reguladas no citado preceito, com as necessárias adaptações às especificidades das ações encobertas *online*.

[61] Também a Lei n.º 144/99, de 31 de agosto, no seu art. 160.º-B, prevê a possibilidade de funcionários de investigação criminal de outros Estados poderem realizar ações encobertas em Portugal com estatuto idêntico aos funcionários de investigação criminal portugueses, mediante autorização do Juiz do Tribunal Central de Investigação Criminal, precedido de proposta do Magistrado do Ministério Público junto do Departamento Central de Investigação e Ação Penal.

[62] Para onde remete o art. 19.º, n.º 1, da Lei n.º 109/2009.

7.1 CATÁLOGO DE CRIMES

Nos termos do art. 19.º, n.º 1, da Lei n.º 109/2009, as autoridades só poderão lançar mão das ações encobertas *online* quando estiver em causa a investigação de[63]:

a) crimes previstos nos arts. 3.º a 8.º da Lei n.º 109/2009 (e outros crimes que venham a ser introduzidos neste diploma);

b) crimes puníveis com pena de prisão de máximo superior a cinco anos que sejam cometidos por meio de um sistema informático; e

c) independentemente da pena aplicável, crimes dolosos contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, burla qualificada, burla informática e nas comunicações, discriminação racial, religiosa ou sexual, os crimes previstos no Título IV do Código do Direito de Autor e dos Direitos Conexos e infrações económico-financeiras quando sejam cometidos por meio de um sistema informático.

7.2 A CUMULAÇÃO COM OUTROS MEIOS DE OBTENÇÃO DA PROVA

Resulta do art. 19.º, n.º 2, da Lei n.º 109/2009 que é admissível cumular as ações encobertas em ambiente informático-digital com a utilização de meios técnicos (com possibilidade de inclusão de uma busca *online*). O que se justifica, visto que, pelo conhecimento

[63] MESQUITA (2010, p. 126) considera que a possibilidade de aplicar este método "oculto" a crimes como os previstos nos arts. 3.º, n.º 1, 5.º, n.ºs 1 e 2, 6.º, n.ºs 1 e 3, e 7.º, n.ºs 1 e 2, da Lei n.º 109/2009, aos crimes dolosos puníveis com penas inferiores a 5 anos de prisão referidos no art. 19.º, n.º 1, al. b), e aos crimes negligentes que sejam puníveis com pena superior a 5 anos de prisão é inconstitucional; também ALBUQUERQUE, 2011, p. 681-682, critica a amplitude do catálogo, propondo uma redução teleológica do mesmo.

empírico adquirido, o êxito da investigação de determinados tipos de criminalidade (*v.g.,* no caso da criminalidade organizada e económico-financeira e do terrorismo) passa pelo uso cumulativo de meios de obtenção de prova altamente restritivos de direitos fundamentais, incluindo as ações encobertas.

No que tange à cumulação com outros meios de obtenção de prova não subsumíveis ao art. 19.º, n.º 2, da Lei n.º 109/2009, nada o impede, sem prejuízo de, no caso concreto, essa cumulação, jamais poder violar os ditames do princípio da proporcionalidade na vertente de proibição do excesso (cfr. ANDRADE, 2009a, p. 115). Significa que essa cumulação nunca poderá conduzir a uma "vigilância total" (*i. e.,* à obtenção, de forma prolongada no tempo e através do uso de medidas de observação, de informações relativas à totalidade da vida do visado, construindo-se, desse modo, um "*umfassendes Persönlichkeitsbild*") (cfr. WOLTER, 2004, p. 745, nota 61), embora, na nossa perspetiva, a eventual existência de "vigilância total" deva ser aferida à luz da situação concreta e não em abstrato.

7.3 O "INTERROGATÓRIO" DO ARGUIDO E/OU DE PESSOAS QUE POSSAM RECUSAR A PRESTAÇÃO DE DEPOIMENTO PELO AGENTE INFILTRADO SEM OS ADVERTIR DA FACULDADE DE NÃO PRESTAREM DECLARAÇÕES

De acordo com os arts. 61.º, n.º 1, al. d), 141.º, n.º 4, als. a) e b), 143.º, n.º 2, 144.º, n.º 2, e 343.º, n.º 1, *in fine*, do CPP, o arguido, antes de prestar declarações acerca dos factos que lhe são imputados, deve ser informado de que goza do direito a não prestar declarações acerca desses factos, sob pena de inutilizabilidade dessas declarações como prova, nos termos do art. 58.º, n.º 5, do CPP.

As pessoas adstritas ao dever de guardar segredo profissional estão obrigadas a não prestar depoimento relativamente a questões

que tenham a ver com o exercício da sua profissão, pelo que, se se recusarem a depor com esse fundamento e, caso a recusa seja legítima, só terão de o prestar no caso de quebra do sigilo profissional nos termos do art. 135.º do CPP.

Também as pessoas referidas no art. 134.º do CPP[64] terão de ser advertidas da faculdade de não prestarem depoimento, sob pena de o seu depoimento não poder ser valorado como prova.

Do mesmo modo, a testemunha, o assistente e as partes civis podem recusar-se a responder a perguntas de que possa resultar a sua responsabilidade penal (cfr. arts. 132.º, n.º 2, e 145.º, n.º 3, do CPP).

E, por fim, as autoridades estão obrigadas a constituir como arguido qualquer pessoa que esteja numa das situações previstas no art. 58.º, n.º 1, do CPP ou que se encontre na situação a que alude o art. 59.º, n.º 2, do CPP e solicite a sua constituição como arguida.

Estas normas visam o interrogatório formal no âmbito de um processo penal, não sendo, pelo menos diretamente, aplicáveis aos "interrogatórios" realizados pelo agente infiltrado, que, pelo seu caráter informal, poderão levar o interlocutor a fornecer informações autoincriminatórias ou cujo fornecimento poderia validamente recusar num interrogatório formal. Todavia, é controversa a admissibilidade da utilização probatória de tais informações (cfr. NUNES, 2019, p. 874 e ss., com vastas indicações doutrinais e jurisprudenciais).

No entanto, apesar de poderem ser fornecidas informações que, no âmbito de um interrogatório formal, poderiam não o ser, consideramos que tais informações poderão ser utilizadas como prova, pois, em primeiro lugar, ainda que o "depoente" desconheça

[64] Os descendentes, os ascendentes, os irmãos, os afins até ao 2.º grau, os adotantes, os adotados e o cônjuge do arguido, bem como quem tiver sido cônjuge do arguido ou quem, sendo de outro ou do mesmo sexo, com ele conviver ou tiver convivido em condições análogas às dos cônjuges, relativamente a factos ocorridos durante o casamento ou a coabitação.

a qualidade do agente infiltrado e as suas finalidades, a atuação do agente infiltrado assenta precisamente em, ocultando a sua qualidade e finalidades, ver e ouvir o que acontece à sua volta (incluindo os "depoimentos" destas pessoas) (cfr. KÖHLER, 2019, p. 524; LIAÑO FONSECA-HERRERO, 2004, p. 222; ELLBOGEN, 2004, p. 93).

Em segundo lugar, não se trata de um expediente para "contornar" as regras do interrogatório formal e o princípio *nemo tenetur se ipsum accusare* (contra, ROXIN, 1997, p. 18 e ss.; ANDRADE, 2009b, p. 544-54) pois o recurso a agentes infiltrados tende a ocorrer antes de o arguido e as testemunhas que possam recusar-se a depor serem ouvidos.

Em terceiro lugar, não estando o agente infiltrado obrigado a informar essas pessoas dos seus direitos processuais nem da sua qualidade e finalidades, não ocorre qualquer fornecimento de elementos falsos acerca de depoimentos ou outros elementos fácticos existentes nos autos para determinar o interrogado a modificar as suas declarações e, como tal, estamos no âmbito da astúcia (cfr. LAMMER, 1992, p. 110 e ss., 119 e 169-170).

Em quarto lugar, exigir que o agente infiltrado advirta tais pessoas da sua qualidade e finalidades e da imputação e direitos processuais não é compatível com a (necessária) natureza "oculta" da ação encoberta e poria em causa a eficácia da diligência e, sobretudo, a segurança do agente (cfr. GERCKE, 2012, p. 585).

Em quinto lugar, a pessoa que "confidencia" ao agente infiltrado está livre na sua pessoa e fora de qualquer coerção decorrente de estar a prestar depoimento perante uma autoridade[65], sendo livre de fazer, ou não, tais "confidências", tudo se assemelhando a uma qualquer conversa em que uma pessoa, confiando no seu interlocutor, lhe confidencia a prática de um crime e este denuncia o facto às

[65] Cfr. ELLBOGEN (2004, p. 89-90), e Acórdão Bykov c. Rússia do Tribunal Europeu dos Direito Humanos. *in https://hudoc.echr.coe.int*.

autoridades[66].

E, em sexto lugar, o *nemo tenetur* não tutela "descuidos" do arguido ou do suspeito (cfr. OTT, 2008, p. 74; LAMMER, 1992, p. 110 e ss.; ELLBOGEN, 2004, p. 89 e ss.; contra, ROXIN, 1997, p. 19-20) nem é absoluto, estando sujeito às restrições necessárias para salvaguardar interesses superiores.

7.4 O DEPOIMENTO DO AGENTE INFILTRADO. O RELATO DA AÇÃO ENCOBERTA

Nos termos do art. 4.º, n.º 3, da Lei n.º 101/2001, oficiosamente ou a requerimento da Polícia Judiciária, a autoridade judiciária competente (que, no inquérito, será o Magistrado do Ministério Público e, na instrução, o Juiz de Instrução Criminal) pode, mediante decisão fundamentada, autorizar que o agente infiltrado, quando atue com identidade fictícia, preste depoimento sob essa identidade no processo relativo aos factos objeto da sua atuação, como forma de proteção do agente infiltrado (e dos seus familiares) contra eventuais pressões e represálias por parte dos arguidos/suspeitos e para permitir a utilização daquele agente em futuras investigações (cfr. NUNES, 2019, p. 882).

Iguais finalidades presidem ao regime previsto no n.º 4 do mesmo preceito, no qual se prevê que, quando o Juiz, por indispensabilidade da prova, determinar a comparência do agente infiltrado na audiência de julgamento, esta deverá decorrer *sempre* com exclusão de publicidade nos termos do art. 87.º, n.º 1, 2.ª parte, do CPP, havendo que aplicar o disposto na Lei n.º 93/99, de 14 de julho. Embora a medida de reserva do conhecimento da identidade da testemunha não seja de aplicação automática (carecendo de decisão fundamentada do Juiz) (assim, NUNES, 2019, p. 882-883),

[66] Cfr. ELLBOGEN (2004, p. 91) e Acórdão Bykov c. Rússia do Tribunal Europeu dos Direito Humanos, *in https://hudoc.echr.coe.int*; contra, ROXIN (1995, p. 465), e LIAÑO-FONSECA HERRERO, 2004, p. 222.

o agente infiltrado prestará tendencialmente o seu depoimento sem que a sua identidade seja revelada e com recurso à ocultação de imagem, distorção de voz e videoconferência (cfr. NUNES, 2019, p. 882). Pois só assim será possível salvaguardar a possibilidade de voltar a utilizar aquela pessoa noutras ações encobertas e proteger essa pessoa e os seus familiares de represálias. No caso do agente infiltrado *online*, ainda que não se coloque a questão da possibilidade de voltar a utilizar aquela pessoa noutras ações encobertas (podendo sempre utilizar um outro *nickname*, ainda que podendo ser necessário criar uma nova "pegada digital"), continuará a, tal como nas ações encobertas "clássicas", colocar-se a questão da proteção da vida e da integridade física do agente infiltrado e dos seus familiares (contra, RAMOS, 2017, p. 79).

Relativamente ao valor probatório do depoimento do agente infiltrado, nos termos do disposto no art. 19.º, n.º 2, da Lei n.º 93/99, nenhuma condenação poderá assentar, exclusiva ou decisivamente, no depoimento ou nas declarações produzidas por uma ou mais testemunhas cuja identidade não foi revelada, pelo que o depoimento de um ou mais agentes infiltrados jamais poderá fundar, exclusiva ou decisivamente, qualquer decisão condenatória (para uma crítica a esta solução legal, *vide* NUNES, 2019, p. 884 e ss.).

Passando ao relato da ação encoberta, de acordo com os arts. 3.º, n.º 6, e 4.º, n.ºs 1 e 2, da Lei n.º 101/2001, a PJ terá de elaborar, no prazo de 48 horas contadas do termo da ação, o relato da ação encoberta, que só será junto ao processo penal se a autoridade judiciária considerar a inquirição do agente infiltrado absolutamente indispensável em termos probatórios.

7.5 O COMETIMENTO DE CRIMES PELO AGENTE INFILTRADO

No decurso da ação encoberta *online*, o agente infiltrado poderá ter de cometer crimes para assegurar o êxito da investigação

(pois precisa de ganhar a confiança dos visados) ou evitar um crime mais grave. No âmbito da atuação do agente infiltrado *online*, é pensável a partilha de pornografia infantil num dado *chat* (que terá de estar relacionado com a partilha de pornografia infantil[67]) ou o fornecimento aos visados de informações sigilosas relativas a investigações em curso, com a finalidade de ganhar a confiança dos demais participantes ou de, por essa via, instalar *benware*[68] nos sistemas informáticos dos visados para levar a cabo, por exemplo, buscas *online*.

O legislador, entendendo que, em determinados casos, será admissível que o agente infiltrado cometa crimes no âmbito da ação encoberta sem incorrer em responsabilidade criminal, previu, no art. 6.º, n.º 1, da Lei n.º 101/2001, uma causa de justificação (neste sentido, ALBUQUERQUE, 2011, p. 686; VALENTE, 2010, p. 557; PINTO, 2013, p. 746; NUNES, 2019, p. 893.). E, nos casos em que o art. 6.º, n.º 1, da Lei n.º 101/2001 não permita excluir a ilicitude da conduta do agente infiltrado, será possível recorrer a causas de justificação, exclusão da culpa ou da punibilidade gerais para afastar a punição (cfr. NUNES, 2019, p. 893).

Para que ocorra a exclusão da ilicitude nos termos do art. 6.º da Lei n.º 101/2001, a prática de atos preparatórios ou de execução de uma infração deverá constituir um meio adequado e necessário à prossecução das finalidades da ação encoberta, deverá ser razoável impor ao lesado o sacrifício do seu interesse face à natureza ou ao valor do interesse ameaçado e o interesse a salvaguardar terá de ser superior ao interesse sacrificado (cfr. PEREIRA, 2004, p. 36-37; NUNES, 2019, p. 893). Tais requisitos são cumulativos.

[67] Caso contrário, poderemos estar perante uma conduta de provocação ao crime.

[68] Por oposição ao *malware* (*malicious software*: *software* malicioso), que visa finalidades ilícitas, o *benware* (*benign software*: *software* benigno), que consiste em programas informáticos similares aos que são utilizados como *malware*, visa interesses legítimos, como sejam a prevenção e a repressão criminais.

No que concerne às formas de comparticipação criminosa que o agente infiltrado poderá adotar, a Lei exclui inequivocamente a autoria mediata e a instigação, não se levantando dúvidas quanto à admissibilidade da coautoria e da cumplicidade (cfr. MEIREIS, 1999, p. 164). No entanto, poderão surgir algumas dúvidas relativamente à autoria material, devendo a análise ser casuística, pois, ainda que o legislador não exclua a autoria material no art. 6.º, n.º 1, da Lei n.º 101/2001 e o agente infiltrado nem sempre execute o crime conjuntamente com outros indivíduos (tudo dependendo das instruções recebidas), se cometer um crime por sua livre iniciativa, a ilicitude não será excluída por via do art. 6.º, n.º 1, da Lei n.º 101/2001, dado que a finalidade da atuação do agente infiltrado é a recolha de provas e não o cometimento de crimes por sua iniciativa (assim, MEIREIS, 1999 p. 164, nota 36; NUNES, 2018, p. 221).

7.6 AS PESSOAS QUE PODERÃO SER ALVO DE AÇÕES ENCOBERTAS *ONLINE*. AS PESSOAS QUE PODEM RECUSAR-SE VALIDAMENTE A DEPOR

Quanto às pessoas cujos dados poderão ser obtidos por via do recurso às ações encobertas *online*, consideramos que haverá que aplicar analogicamente o art. 187.º, n.º 4, do CPP, por imposição do princípio da proporcionalidade na vertente de proibição do excesso, dado que se nos afigura que a sua utilização dificilmente será útil relativamente a outros alvos que não o arguido, o suspeito, o intermediário ou a vítima (neste caso, mediante consentimento) e, para além disso, estamos perante um meio de obtenção de prova altamente restritivo de direitos fundamentais e inclusivamente mais lesivo do que as escutas telefónicas (cfr. NUNES, 2018, p. 222).

Passando às pessoas que se possam recusar validamente a depor, quanto às pessoas sujeitas ao segredo religioso e de Estado, gozando tais segredos de uma tutela absoluta (cfr. arts. 135.º, n.ºs 1

e 5, e 137.º do CPP), não poderão valorar-se as informações obtidas cujo conteúdo esteja abrangido por algum desses segredos.

Relativamente às pessoas obrigadas a guardar sigilo profissional e começando pela situação do defensor, apesar de o regime das ações encobertas não conter qualquer norma similar ao art. 187.º, n.º 5, do CPP, ainda assim consideramos que, pela necessidade de salvaguardar o exercício cabal do direito de defesa, não poderão ser valoradas as provas obtidas no âmbito de uma ação encoberta mediante a ingerência nas relações entre o arguido e o defensor, *salvo* se constituírem ou existirem razões para crer que essas relações constituem objeto ou elemento de um crime. Quanto às demais pessoas sujeitas ao dever de guardar segredo profissional, a valoração de tais provas não é proibida, não sendo aplicável o regime do art. 187.º, n.º 5, do CPP (cfr. NUNES, 2018, p. 223 e 184 e ss., com argumentos e indicações bibliográficas), sem prejuízo de dever considerar-se a circunstância de poderem ser obtidas informações protegidas pelo sigilo profissional em sede de ponderação no momento de autorizar a realização da ação encoberta.

Por fim, quanto às pessoas que, por via de especiais relações com o arguido, têm o direito a recusar a prestação de depoimento nos termos do art. 134.º do CPP, não há que aplicar, ainda que analogicamente, o regime do art. 187.º, n.º 5, do CPP (assim, NUNES, 2018, p. 223 e 186 e ss., com argumentos e indicações bibliográficas).

7.7 A COMPETÊNCIA AUTORIZATIVA

De acordo com o art. 3.º, n.ºs 3 a 5, da Lei n.º 101/2001, a competência autorizativa é do Magistrado do Ministério Público (quando ocorram no âmbito de um inquérito) ou do Juiz de Instrução Criminal que exerça funções no Tribunal Central de Instrução Criminal (quando ocorram na prevenção criminal), sendo o art. 19.º da Lei n.º 109/2009 omisso a este respeito.

As ações encobertas constituem uma restrição de direitos fundamentais particularmente intensa, pelo que, por imposição do art. 32.º, n.º 4, da Constituição da República Portuguesa, o recurso às ações encobertas insere-se na reserva de Juiz (cfr. ALBUQUERQUE, 2011, p. 683; RODRIGUES, 2010, p. 126; NUNES, 2019, p. 902). No entanto, o regime do art. 3.º, n.º 3, da Lei n.º 101/2001, não viola a Constituição, uma vez que, ainda que a reserva de Juiz se deva à necessidade da intervenção prévia por parte de uma entidade "neutra" para obstar à existência de arbítrio na limitação dos direitos fundamentais e que, como tal, fosse preferível uma autorização prévia do Juiz de Instrução Criminal, a sua intervenção *a posteriori* ainda permite observar a imposição do art. 32.º, n.º 4, da Constituição (cfr. VALENTE, 2010, p. 551; NUNES, 2019, p. 902-903; RODRIGUES, 2010, p. 126).

Contudo, consideramos que o art. 3.º, n.º 3, da Lei n.º 101/2001, na parte em que admite a ratificação tácita do Juiz de Instrução Criminal, é inconstitucional (por violação do art. 32.º, n.º 4, da Constituição), na medida em que, aí sim, as finalidades da reserva de Juiz não são prosseguidas, pois o legislador permite que uma restrição intensa de direitos fundamentais possa ocorrer sem qualquer ponderação judicial ou meramente com uma ficção ou presunção de ponderação judicial (assim, VALENTE, 2009, p. 172; RODRIGUES, 2010, p. 126; NUNES, 2019, p. 903; contra, RAMOS, 2017, p. 45, nota 64).

A omissão da comunicação ao Juiz de Instrução Criminal configura uma nulidade (sanável, nos termos do art. 120.º, n.º 2, al. d), do CPP), sendo que, pelas razões aduzidas supra, a confirmação, pelo Juiz, terá de ser expressa, pois o art. 3.º, n.º 3, da Lei n.º 101/2001, na parte em que admite a confirmação tácita, é inconstitucional.

Outra reserva que o regime vigente nos suscita prende-se com o facto de não detetarmos quaisquer diferenças em termos de ingerência nos direitos fundamentais entre a prevenção criminal e

a repressão criminal que possam justificar a adoção de um regime autorizativo diverso ao nível da competência.

Por fim, nos termos do art. 19.º, n.º 2, sempre que seja necessário recorrer a meios e dispositivos informáticos no âmbito da ação encoberta, essa utilização depende de autorização judicial, ainda que a entidade competente para autorizar a ação encoberta no caso concreto seja o Ministério Público.

8 CONCLUSÕES

1. O cibercrime é filho do extraordinário desenvolvimento tecnológico das últimas décadas ao nível da informática e das comunicações.
2. Esse desenvolvimento tecnológico, a par dos aspetos positivos, trouxe igualmente aspetos negativos, pois os novos instrumentos que "disponibilizou" também podem ser usados para fins ilícitos, incluindo a preparação, a execução e o apagamento das provas com cometimento de crimes (inclusivamente de crimes graves como atos terroristas, tráfico de droga/armas/seres humanos/órgãos, homicídios, abuso sexual de crianças e difusão de pornografia infantil, espionagem, destruição ou danificação de infraestruturas críticas e branqueamento de capitais.
3. O cibercrime é uma forma de crime transnacional em evolução e uma realidade complexa, decorrendo essa complexidade: (1) do facto de ocorrer no território incomensurável, imaterial e sem fronteiras do Ciberespaço e (2) do crescente envolvimento de organizações criminosas e terroristas e de criminosos de colarinho branco.
4. A utilização dos meios informáticos permite (1) apagar as barreiras psicológicas que muitas vezes existem

quando o criminoso tem de encarar a vítima e (2) atingir um número elevado de pessoas em todo o Mundo com grande facilidade e rapidez, (3) dificulta a localização e a identificação dos criminosos e a recolha de provas (por via do aproveitamento da rapidez, anonimato e volatilidade das comunicações informáticas e da utilização de medidas antiforenses, como a encriptação de mensagens, a esteganografia, a utilização de *firewalls*, *Botnets*, VPN ou *proxies*, da *Dark Web*, de programas como o Tor, *Freenet* e I2P e de criptomoedas, etc.).

5. Ciente de toda esta realidade e da necessidade de adequar a Lei processual penal, o Conselho da Europa adotou a Convenção sobre o Cibercrime do Conselho da Europa, aberta à assinatura em Budapeste em 23 de novembro de 2001, na qual preveem vários meios de obtenção de prova específicos para a obtenção de prova digital.

6. O legislador português transpôs essa Convenção para a ordem jurídica portuguesa através da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que inclui, nos artigos 12.º a 19.º, vários meios de obtenção de prova específicos para a obtenção de prova digital (os previstos na Convenção de Budapeste e mais s dois, embora essa Lei não esgote os meios de obtenção de prova relativos à prova digital: as perícias e os exames estão previstos e regulados no CPP).

7. Um desses meios são as ações encobertas *online,* de que nos ocupamos no presente artigo.

8. As ações encobertas *online* têm-se mostrado úteis na resposta ao jogo ilícito, ao tráfico de estupefacientes, à pornografia infantil e à pedofilia *online*, ao tráfico de armas e ao branqueamento de capitais.

9. Nas investigações na *Dark Web*, a integração do agente infiltrado numa comunidade *online* e a sua interação com criminosos pertencentes a essa comunidade permitem neutralizar os obstáculos criados por via da utilização de técnicas antiforenses, descobrir a identidade e a localização dos autores dos crimes e a recolha de provas dos crimes através da persuasão dos próprios suspeitos a cederem tais informações.

10. A eficácia da ação encoberta pode ser potenciada através da utilização de meios ou dispositivos informáticos (*v.g.,* realizando uma busca *online*).

11. O legislador português define ação encoberta no art. 1.º, n.º 2, da Lei n.º 101/2001 como "aquela que seja desenvolvida 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".

12. A Lei portuguesa permite o uso de *Cybercops*, sendo as provas obtidas lícitas, apenas havendo que dar cumprimento ao disposto no art. 19.º, n.º 2, da Lei n.º 109/2009.

13. Ao nível das ações "encobertas", encontramos diversos tipos "atores" (agente encoberto, agente infiltrado, agente provocador e "homem de confiança").

14. Apenas o agente infiltrado e o "homem de confiança" quando a sua atuação seja subsumível ao conceito de agente infiltrado estão sujeitos ao regime jurídico das ações encobertas, sendo a atuação do agente encoberto um meio de obtenção de prova atípico admissível à luz do art. 125.º do CPP e a atuação do agente provocador um método proibido de prova nos termos do art. 126.º,

n.º 2, al. a), do CPP, por violar as garantias fundamentais do processo penal.

15. Nos termos do art. 19.º, n.º 1, da Lei n.º 109/2009, as autoridades só poderão lançar mão das ações encobertas em ambiente informático-digital quando estiver em causa a investigação de um dos crimes aí previstos.

16. O art. 19.º, n.º 2, da Lei n.º 109/2009 permite cumular as ações encobertas *online* com a utilização de meios técnicos (onde se poderá incluir uma busca *online*) e, pelo conhecimento empírico adquirido, o êxito da investigação de determinados tipos de criminalidade exige o uso cumulativo de meios de obtenção de prova altamente restritivos de direitos fundamentais, onde se incluem as ações encobertas. Nada impede essa cumulação, desde que estejam verificados os pressupostos de cada um desses meios de obtenção de prova e essa cumulação, em concreto, não viole o princípio da proporcionalidade, não podendo jamais ocorrer a uma "vigilância total".

17. São admissíveis como prova as declarações do agente infiltrado na parte em que se refiram a informações que lhe tenham sido "fornecidas" pelo arguido ou por pessoas que possam recusar a prestação de depoimento sem terem sido advertidos da qualidade e finalidades prosseguidas pelo agente infiltrado.

18. O agente infiltrado prestará tendencialmente o seu depoimento sem que a sua identidade seja revelada e com recurso à ocultação de imagem, distorção de voz e videoconferência, embora, nos termos do art. 19.º, n.º 2, da Lei n.º 93/99, nenhuma condenação possa assentar, exclusiva ou decisivamente, no depoimento de um ou mais agentes infiltrados, precisamente porque o seu depoimento foi prestado nas referidas condições.

19. No decurso da ação encoberta *online*, o agente infiltrado poderá ter de cometer crimes para assegurar o êxito da investigação ou evitar um crime mais grave, sendo a ilicitude da sua conduta excluída sempre que estejam verificados os pressupostos da causa de justificação prevista no art. 6.º, n.º 1, da Lei n.º 101/2001 e, nos casos em que tal não seja possível, se estiverem verificados os pressupostos de uma qualquer outra causa de justificação, de exclusão da culpa ou da punibilidade "gerais", o agente não será punido.

20. Por imposição do princípio da proporcionalidade só é admissível utilizar ações encobertas visando o arguido, o suspeito, o intermediário ou a vítima (neste caso, mediante consentimento), havendo que aplicar analogicamente o art. 187.º, n.º 4, do CPP (relativo às escutas telefónicas).

21. Pela necessidade de salvaguardar o exercício cabal do direito de defesa, não podem ser valoradas as provas obtidas no âmbito de uma ação encoberta mediante a ingerência nas relações entre o arguido e o defensor, *salvo* se existirem razões para crer que essas relações constituem objeto ou elemento de um crime.

22. Nada impede a utilização de provas obtidas no âmbito de uma ação encoberta relativamente a pessoas sujeitas ao dever de guardar segredo profissional sem prévia quebra do sigilo profissional ou a pessoas que, por via de especiais relações com o arguido, têm o direito a recusar a prestação de depoimento sem serem previamente advertidas de que têm esse direito.

23. A competência para autorizar as ações encobertas *online* é do Magistrado do Ministério Público (quando ocorram no âmbito de um inquérito) ou do Juiz de Instrução Criminal

que exerça funções no Tribunal Central de Instrução Criminal (quando ocorram na prevenção criminal).

24. As ações encobertas constituem uma restrição de direitos fundamentais particularmente intensa, pelo que se inserem na reserva de Juiz; todavia, o art. 3.º, n.º 3, da Lei n.º 101/2001, na parte em que atribui a competência autorizativa ao Ministério Público não é inconstitucional, pois, a intervenção judicial *a posteriori* ainda permite observar a imposição do art. 32.º, n.º 4, da Constituição.

25. No entanto, o art. 3.º, n.º 3, da Lei n.º 101/2001 é inconstitucional (por violação do art. 32.º, n.º 4, da Constituição) na parte em que admite a ratificação tácita do Juiz, pois permite que uma restrição intensa de direitos fundamentais possa ocorrer sem qualquer ponderação judicial ou meramente com uma presunção de ponderação judicial.

BIBLIOGRAFIA

ABADINSKY, Howard. **Organized crime**. 9. ed. Belmont: Wadsworth Cengage, 2007.

ALBANESE, Jay S. **Organized crime in our times**. 5. ed. Newark: Matthew Bender, 2007.

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

ANDRADE, Manuel da Costa. **Bruscamente no verão pasado**: a reforma do código de processo penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra: Coimbra Ed., 2009a.

ANDRADE, Manuel da Costa. Das escutas telefónicas. In: I Congresso de Processo Penal. **Memórias**... Coimbra: Almedina, 2005. p. 215 e ss.

ANDRADE, Manuel da Costa. Métodos ocultos de investigação (plädoyer para uma teoria geral). In: MONTE, Mário Ferreira (Coord.). **Que futuro para o direito processual penal**: simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do código de processo penal português. Coimbra: Coimbra Ed., 2009b. p. 525 e ss.

ANDRADE, Manuel da Costa. **Sobre as proibições de prova em processo penal**. Coimbra: Coimbra Ed., 1992.

BRITO, Maria Beatriz Seabra de. **Novas tecnologias e legalidade da prova em processo penal**. Coimbra: Almedina, 2018.

CAMPOS, Juliana Filipa Sousa. **O *malware* como meio de obtenção de prova em processo penal**. Coimbra: Almedina, 2021.

CONCEIÇÃO, Ana Raquel. **Escutas telefónicas**: regime processual penal. Lisboa: Quid Juris, 2009.

CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter. In: **Revista do Ministério Público**, Lisboa, Ed. Sindicato dos Magistrados do Ministério Público, n.º 139, p. 29 e ss., 2014.

CUNHA, José Manuel Damião da. O regime legal das escutas telefónicas: algumas breves reflexões. In: **Revista do Centro de Estudos Judiciários**, (Especial) Jornadas sobre a revisão do Código de Processo Penal, Lisboa, Centro de Estudos Judiciários, número 9, p. 205 e ss, 2008.

ELLBOGEN, Klaus. **Die verdeckte ermittlungstätigkeit der strafverfolgungsbehörden durch zusammenarbeit mit**

V-Personen und informanten. Berlim: Duncker & Humblot, 2004.

FIDALGO, Sónia. A utilização de inteligência artificial no âmbito da prova digital: direitos fundamentais (ainda mais) em perigo. In: MIRANDA, Anabela Miranda (Coord.). **A inteligência artificial no direito penal**, pp. 129 e ss. Coimbra: Almedina, 2020.

GERCKE, Björn. §110c. In: GERCKE, Björn; JULIUS, Karl-Peter; TEMMING, Dieter (Hrsg.). **Heidelberger kommentar**: zur strafprozessordnung, 5. ed. Heidelberg: C. F. Müller, 2012. p. 584 e ss.

GLENNY, Misha. **Darkmarket**: como os hackers se tornaram a nova máfia. Lisboa: Civilização, 2012.

JESUS, Francisco Marcolino de. **Os meios de obtenção de prova em processo penal**. Coimbra: Almedina, 2011.

KÖHLER, Marcus. §110c. In: MEYER-GOßNER, Lutz; SCHMITT, Bertram. **Strafprozessordnung mit GVG und nebengesetzen**. 62. ed. Munique: C. H. Beck, 2019. p. 523-524.

LAMMER, Dirk. **Verdeckte ermittlungen im strafprozeß**: zugleich eine studie zum menschenwürdegehalt der grundrechte. Berlim: Duncker & Humblot, 1992.

LEITE, André Lamas. As escutas telefónicas: algumas reflexões em redor do seu regime e das consequências processuais derivadas da respectiva violação. In: Separata da **Revista da Faculdade de Direito da Universidade do Porto**, Coimbra, Coimbra Ed., ano I, p. 9 e ss, 2004.

LIAÑO-FONSECA HERRERO, Marta Gómez de. **Criminalidad organizada y medios extraordinarios de investigación**. Madrid: Colex, 2004.

MEIREIS, Manuel Augusto Alves. **O regime das provas obtidas pelo agente provocador em processo penal**. Coimbra: Almedina, 1999.

MESQUITA, Paulo Dá. **Processo penal, prova e sistema judiciário**. Coimbra: Coimbra Ed., 2010.

NACK, Armin. §110a. In: HANNICH, Rolf (Ed.). **Karlsruher kommentar zur strafprozessordnung mit GVG, EGGVG und EMRK**. 6. ed. Munique: C. H. Beck, 2008. p. 540 e ss.

NEVES, Rita Castanheira. **As ingerências nas comunicações electrónicas em processo penal**: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova. Coimbra: Coimbra Ed., 2011.

NUNES, Duarte Rodrigues. Da admissibilidade da utilização de *benware* no direito portugués. In: Ciberlaw, n.º 10 (setembro-dezembro de 2020a), p. 10 e ss. Disponível em: <https://www.cijic.org/publicacao/da-admissibilidade-da-utilizacao-de-benware-no-direito-portugues/>. Acesso em: 28 jun. 2021.

NUNES, Duarte Rodrigues. O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada (Tese de Doutoramento). Coimbra: Gestlegal, 2019.

NUNES, Duarte Rodrigues. **Os crimes previstos na lei do cibercrime**. Coimbra: Gestlegal, 2020b.

NUNES, Duarte Rodrigues. **Os meios de obtenção de prova previstos na lei do cibercrime**. Coimbra: Gestlegal, 2018.

OTT, Katharina. **Verdeckte ermittlungen im strafverfahren**: die deutsche rechtsordnung und die rechtslage nach der EMRK in einer rechtsvergleichenden betrachtung. Frankfurt: Peter Lang, 2008.

PEREIRA, Rui. O "agente encoberto" na ordem jurídica portuguesa. In: **Medidas de combate à criminalidade organizada e económico-financeira.** Lisboa: Centro de Estudos Judiciários / Coimbra Ed., 2004. p. 11 e ss.

PINHO, Carlos. Os problemas interpretativos resultantes da lei n.º 32/2008, de 17 de julho. In: **Revista do Ministério Público**, Lisboa, Ed. Sindicato dos Magistrados do Ministério Público, n.º 129, p. 63 e ss., 2012.

PINTO, Frederico de Lacerda da Costa. **A categoria da punibilidade na teoria do crime**. t. II. Coimbra Almedina, 2013.

PINTO PALACIOS, Fernando; PUJOL CAPILLA, Purificación. **La prueba en la era digital**. Madrid: Wolters Kluwer, 2017.

PORTUGAL. Tribunal da Relação de Évora. Acórdão de 6 de janeiro de 2015 (Processo 6793/11.6TDLSB-A.E1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Évora. Acórdão de 20 de janeiro de 2015 (Processo 648/14.6GCFAR-A.E1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 3 de maio de 2016 (Processo 73/16.4PFCSC-A.L1-5). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 7 de março de 2017 (Processo 1585/16.5PBCSC-A.L1-5). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação do Porto. Acórdão de 13 de abril de 2016 (Processo 471/15.0T9AGD-A.P1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação do Porto. Acórdão de 5 de abril de 2017 (Processo 671/14.0GAMCN.P1). Disponível em: <www.dgsi.pt>.

RAMALHO, David Silva. A investigação criminal na Dark Web. In: **Revista de Concorrência e Regulação**, Coimbra, Ed. Almedina, ano IV, n.ºs 14-15, p. 383 e ss., 2013a.

RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital**. Coimbra: Almedina, 2017.

RAMALHO, David Silva. O uso de *malware* como meio de obtenção de prova em processo penal. In: **Revista de Concorrência e Regulação**, Coimbra, Ed. Almedina, ano IV, n.º 16, p. 195 e ss., 2013b.

RAMOS, Armando Reis Dias. **A prova digital em processo penal**: o correio eletrónico. Lisboa: Chiado, 2014.

RAMOS, Armando Reis Dias. **O agente infiltrado digital**: contributo para o estudo das vicissitudes da recolha de prova em direito penal informático. Tese de Doutoramento em Direito. Lisboa, 2017.

RODRIGUES, Benjamim Silva. **Da prova penal**: bruscamente... a(s) face(s) oculta(s) dos métodos ocultos de investigação criminal. t. II. Lisboa: Rei dos Livros, 2010.

RODRIGUES, Benjamim Silva. **Das escutas telefónicas**. t. I. 2. ed. Coimbra: Coimbra Ed., 2008.

ROXIN, Claus. Nemo tenetur: die rechtsprechung am scheideweg. In: **Neue Zeitschrift für Strafrecht**, Munique e Frankfurt, C. H. Beck'sche Verlagsbuchhandlung, p. 465 e ss., 1995.

ROXIN, Claus. Zur hörfällen-beschluss des grossen senats für

strafsachen, In: **Neue Zeitschrift für Strafrecht**, Munique e Frankfurt, C. H. Beck'sche Verlagsbuchhandlung, p. 18 e ss., 1997.

ROXIN, Claus; SCHÜNEMANN, Bernd. **Strafverfahrensrecht**. 27. ed. Munique: C.H.Beck, 2012.

SILVA, Germano Marques da. **Curso de processo penal.** v. II. 4. ed. Lisboa: Verbo, 2008.

SOINÉ, Michael. Kriminalistische list im ermittlungsverfahren. In: **Neue Zeitschrift für Strafrecht**, Munique e Frankfurt, C. H. Beck'sche Verlagsbuchhandlung, p. 596 e ss., 2010.

SOINÉ, Michael. Personale verdeckte ermittlungen in sozialen netzwerken zur strafverfolgung. In: **Neue Zeitschrift für Strafrecht**, Munique e Frankfurt, C. H. Beck'sche Verlagsbuchhandlung, p. 248 e ss., 2014.

SUSANO, Helena. **Escutas telefónicas**: exigências e controvérsias do atual regime. Coimbra: Coimbra Ed., 2009.

UNIÃO EUROPEIA. Tribunal Europeu dos Direitos Humanos. Acórdão Bykov c. Rússia (de 10 de março de 2009). Disponível em: <https://hudoc.echr.coe.int>.

VALENTE, Manuel Monteiro Guedes. A investigação do crime organizado. VALENTE, Manuel Monteiro Guedes (Coord). In: **Criminalidade organizada e criminalidade de massa**: interferências e ingerências mútuas. Coimbra: Almedina, 2009. p. 159 e ss.

VALENTE, Manuel Monteiro Guedes. **Escutas telefónicas, da excepcionalidade à vulgaridade**. 2. ed. Coimbra: Almedina, 2008.

VALENTE, Manuel Monteiro Guedes. **Processo penal**. t. I, 3. ed. Coimbra: Almedina, 2010.

VENÂNCIO, Pedro Dias. **Lei do cibercrime**: anotada e comentada. Coimbra: Coimbra Ed., 2011.

VERDELHO, Pedro. A convenção sobre o cibercrime do conselho da Europa: repercussões na lei portuguesa. In: **Direito da Sociedade da Informação**, Coimbra, Ed. Coimbra, v. VI, p. 257 e ss., 2006.

VERDELHO, Pedro. "Cibercrime". In: **Direito da Sociedade da Informação**, Coimbra, Ed. Coimbra, v. IV, p. 347 e ss., 2003.

WOLTER, Jürgen. Potenzial für eine totalüberwachung im strafprozess: und Polizeirecht. In: **Festschrift für Hans-Joachim Rudolphi zum 70**: geburtstag. Neuwied: Luchterhand, 2004. p. 733 e ss.

Recebido em: 13-7-2021
Aprovado em: 16-2-2022