NOTA PRÉVIA

O presente estudo traduz a nossa dissertação de doutoramento, apresentada à Universdidade Autónoma de Lisboa e defendida em 25 de outubro de 2018.

Toda a legislação mencionada encontra-se atualizada até 30 de novembro de 2021.

Introdução

1. Introdução

§1. Nas últimas décadas temos assistido, impávidos e com alguma ansiedade, ao desenvolvimento crescente da tecnologia. Esta ansiedade resulta da forma como a tecnologia ainda nos consegue surpreender no momento em que surgem, à venda no mercado, novidades tecnológicas[1]. Se no início dos anos 90, do século passado, a Internet era uma ferramenta de trabalho, considerada um *luxo*, acessível apenas a um nicho muito restrito de pessoas, essencialmente militares e estudantes universitários, atualmente tal já não procede de tal forma. Aliás, nos dias de hoje cada pessoa transporta nos seus bolsos pequenos computadores, comummente designados por *smartphones*, que servem também para receber e realizar chamadas telefónicas, havendo uma dependência *encoberta*, que só vem à tona quando não se tem rede GSM ou rede *wireless*, ou seja, quando nos cortam o *cordão umbilical* de comunicabilidade com o mundo.

Se as tecnologias são um bem necessário e útil para a vida em sociedade, pela facilidade e rapidez da comunicação, aliado aos baixos custos de transmissão, há também o reverso da utilização desta tecnologia. Esta dualidade sempre existiu na ciência, aproveitando-se as caraterísticas benéficas para se tirar partido destas por formas menos lícitas. Surgiram, deste modo, novas práticas rebuscadas de cometimento de ilícitos criminais, através destas novas ferramentas, em especial através da internet. Paralelamente também assistimos a novos tipos de ilícitos, mas a grande

[1] As notícias sobre as eventuais novidades e fugas de informação relativamente a eventos mundiais sobre tecnologia, tal como p. ex. a que ocorre em setembro da Apple, sucedem-se todos os anos. Após o lançamento dos novos produtos verifica-se um aumento das vendas.

maioria são crimes *velhos* cometidos sob novas formas. Poderemos indubitavelmente afirmar que os criminosos também se adaptaram aos *novos mundos*, recorrendo sem hesitar a instrumentos informáticos que lhes dão uma tríplice vantagem: a desterritorialização da prática criminosa, a rapidez de atuação e a eficácia das ações criminosas sob o manto do anonimato. Aliado a este tríplice fator, encontraram ainda a seu favor um menor risco na prática da sua atividade delitual, ou seja, a de virem eventualmente a ser identificados e, consequentemente, julgados pela justiça. No fundo os cibercriminosos tiram proveito destas novas técnicas, enriquecem à conta de comportamentos delituosos e tentam, a todo o custo, engendrar situações para se furtarem ao cumprimento de sanções privativas da liberdade.

§2. Com estes novos *modus operandi*, de cometimento de ilícitos criminais, surgem, necessariamente, novas formas de investigação que rompem com técnicas e práticas utilizadas até então pelas forças policiais na investigação da criminalidade[2].

Centremos o pensamento, por breves instantes, nos atos hediondos que têm marcado o mundo nos últimos anos. Iniciaremos este trilho mencionando alguns dos principais ataques terroristas: Nova Iorque, nas torres gémeas; donde se seguiriam mais tarde Madrid, estação de caminhos de ferros de Atocha; Londres, no metropolitano; Boston-EUA,

[2] Neste sentido a União Europeia, através do Conselho Europeu de Amesterdão, realizado nos dias 16 e 17 de junho de 1997, aprovou um plano de ação contra a criminalidade organizada, publicado no JOCE n.º C-124, em 3 de maio de 2000, onde se refere que "*A actividade criminosa organizada é dinâmica por natureza, não necessitando de se circunscrever a estruturas rígidas. Já deu provas de que é capaz de espírito de iniciativa e mentalidade empresarial e consegue ser extremamente flexível na forma como responde a forças e situações de mercado em constante mutação.*"
In http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:124:0001:0033:pt:PDF [*acedido em 20 de janeiro de 2015*].
De realçar que já em 2021 a UE, no âmbito da EMPACT (Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas) que define as prioridades em matéria de luta contra a criminalidade grave e organizda para 2022-2025, considerou os ciberataques com a segunda prioridade, entre os 10 tipos de criminalidade grave e organizada a ter em conta neste período. In https://www.consilium.europa.eu/pt/press/press-releases/2021/05/26/fight-against-organised-crime-council-sets-out-10-priorities-for-the-next-4-years/ [*acedido em 07 de junho de 2021*].

aquando da realização de uma maratona; Paris, no jornal satírico *Charlie Hebdo*; mais recentemente na Bélgica, no aeroporto e metro de Bruxelas; e, em Paris, num concerto dado pela banda *Eagles of Death Metal*, entre outros que se lhes seguiram e que foram amplamente noticiados.

Estas ações terroristas não são perfunctórias. Desde a sua génese, conceção e concretização material são levados a cabo procedimentos organizativos até ao ínfimo pormenor, existindo dentro da organização uma hierarquia de funções e escrupulosos procedimentos a adotar. As cúpulas detsas organizações e os mentores criminosos são conhecedores das ferramentas que as autoridades dos diversos países utilizam, quer a nível interno, quer a nível da cooperação interestadual, na investigação deste tipo de criminalidade. Por esse motivo socorrem-se e utilizam todas as formas de anonimato, para que não possam ser descobertos e as suas ações possam ser concretizadas com sucesso.

A criminalidade mais grave é-nos revelada por diversos modos: desde os jornais, passando pelos canais de televisão, até nas redes sociais, etc... Mas não se julgue que o anonimato apenas se encontra presente neste tipo de criminalidade.

As tecnologias de informação e comunicação trouxeram também consigo a faculdade de partilharmos informação. As redes de indivíduos que produzem e partilham conteúdos de índole sexual com menores passaram das salas de conversações, designadas por chats, tais como o mIRC[3] [4] para plataformas mais arrojadas e cada vez mais difíceis de identificar.

[3] Devido à especificidade do tema que iremos discorrer ao longo destas páginas serão utilizados diversos termos informáticos. Pese embora o tema *sub judice* seja exclusivamente jurídico não nos poderemos alhear desta situação e tentaremos, sempre que se justifique, explicar convenientemente os referidos termos que escapam à área do Direito, mas que estão intimamente ligados ao nosso labor académico.

[4] mIRC (*Internet Relay Chat*) foi um dos primeiros programas de conversação, criado em 1995 por Khaled Mardam-Bey, para o sistema da Microsoft Windows. Neste programa poderiam ser encontradas várias "salas" públicas ou privadas em que o utilizador entrava com um *nick-name* ou *aliás* e poderia conversar com qualquer pessoa, em qualquer parte do mundo. O uso deste programa teve o seu declínio com o surgimento de novas formas mais intuitivas de comunicação (salas de conversação em fóruns, surgimento de aplicações destinadas a conversação *online*, etc. Muito recentemente, no decurso de 2011 principalmente, ressuscitou o interesse pela utilizazação massiva deste programa, de um modo especial pelo grupo ativista denominado *Anonymous*, onde dão formação *online* sobre anonimização, formas de proteção

§3. Resulta, deste avanço tecnológico, a necessidade premente de se adotarem meios capazes de investigar os crimes que são cometidos por esta via. As modernas tecnologias assim o exigem pois só desse modo se poderão identificar os autores que praticam crimes atrás de um computador, resguardados de mil e uma técnicas de manutenção do anonimato, visando o lucro instantâneo. Só com uma alteração do paradigma existente se poderá apetrechar os investigadores deste tipo de criminalidade com as mesmas armas que os delinquentes e obter investigações profícuas que levem à descoberta e à consequente punição dos agentes do crime.

Para além das alterações no direito penal objetivo também o direito penal subjetivo têm de se adequar à realidade destes crimes. Nascem assim novos meios de obtenção de prova, que por sua vez nos revelarão a prova digital, tentando apurar a verdade material dos factos e fazer a devida justiça.

§4. Entre os mais diversos *métodos ocultos*[5] de investigação criminal, que designaremos por *meios especiais e técnicos de investigação criminal*,

nas redes informáticas, como entrar em sistemas informáticos e onde planeiam ataques concertados a estruturas informáticas. A título de exemplo informação divulgada em https://anonops.com/mirc.html [*acedido em 20 de janeiro de 2015*].

[5] A expressão não é nossa, diversos autores a utilizam, tais como Costa Andrade, Dá Mesquita, Benjamim Silva Rodrigues, Faria Costa, entre outros.

Concretamente Costa Andrade define métodos ocultos de investigação criminal como sendo "*uma intromissão nos processos de acção, interacção e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto ou dele se apercebam*" donde, "*continuam a agir, interagir, expressar-se e comunicar de forma "*inocente*", fazendo ou dizendo coisas de sentido claramente auto-incriminatório ou incriminatório daqueles que com elas interagem ou comunicam*" *in* Manuel da Costa Andrade, *Bruscamente no Verão Passado – A reforma do Código de Processo Penal, observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, Cit., pp. 105-106.

Efetivamente, com o devido respeito que é muito, não perfilharemos tal expressão por a mesma traduzir uma carga subjetivamente negativa de ilegalidade (ocultar significa: Subtrair às vistas, esconder; Dissimular; Recetar; Sonegar; Calar, não revelar; **"oculto"** *in* Dicionário Priberam da Língua Portuguesa, http://www.priberam.pt/dlpo/oculto [*consultado em 20-11-2015*]), quando na realidade tais métodos de investigação deverão pautar-se sempre e exclusivamente pela transparência e, acima de tudo, pela legalidade da sua obtenção. Donde, com a devida vénia a tão ilustres professores que utilizam a referida expressão, passaremos a

debruçamo-nos sobre a figura do *agente encoberto* nos crimes praticados exclusivamente por intermédio das Redes de Informação e Comunicação. Balizamos o nosso trabalho a esta forma de investigação criminal – o agente encoberto digital – cientes que estaremos a correr um risco desafiante na medida em que, como nos refere Costa Andrade, "*o que é tecnicamente possível não é, só por si e sem mais, legítimo. Só o será se e na medida em que estiver coberto por expressa e inequívoca intervenção do legislador*"[6]. Desafio este que se agudiza com as possibilidades que as tecnologias nos dias de hoje nos oferecem e pelas quais deverão existir legalmente regras mais rígidas de controle da sua utilização, por parte da autoridade judiciária competente para o efeito. Não poderemos olvidar que sem tal fiscalização será mais fácil o atropelo de Direitos, Liberdades e Garantias dos cidadãos, com prejuízo inerente para quem é investigado e esbulhado da sua intimidade.

É sobre estas novas formas de investigação, presentes na legislação processual penal primária ou secundária, que irá assentar o nosso trabalho de investigação. A especificidade dos crimes informáticos ou cometidos por via informática, na sua vertente mais organizada ou altamente organizada, requerem novas e eficazes formas de investigação da criminalidade cada vez mais complexa.

O facto de focalizarmos o nosso âmbito de acção na figura do agente encoberto digital, em deterimento de analisarmos outras formas mais abrangentes de investigação criminal na internet, leva-nos a traçar objetivamente o desejo de contribuir para o repensar de métodos de investigação criminal modernos, adequados aos tempos que vivemos. Teria sido mais fácil, confessamos, ter optado pela primeira via. Teríamos certamente mais sucesso na recolha de elementos de estudo e casos mais abundantes para apreciar e debater juridicamente relativamente às téc-

chamar-lhe *meios especiais e técnicos de investigação criminal*, porque estes, nos quais se incluem as escutas telefónicas, as buscas "*on-line*", dispositivos de escuta direta, interceções de comunicações informáticas, entre outros, dependem exclusivamente das tecnologias para os seus intentos finais.

[6] Manuel da Costa Andrade, *Bruscamente no Verão Passado – A reforma do Código de Processo Penal, observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, pp. 150.

nicas e formas de investigação criminal usadas na criminalidade informática *lato senso*. Ainda assim não preferimos usar o caminho mais fácil, pois este não nos traria a satisfação de aprofundarmos convenientemente os itens todos que abordaríamos e ficaríamos sujeitos a uma análise superficial dada a matéria em causa.

§5. O agente encoberto digital revoluciona toda a forma de investigação que efetivamente pode ser concretizada num processo crime. Há metodologias e métodos novos que as tecnologias informáticas permitem que se usem na recolha de prova, tais como as ações técnicas encobertas, ou seja, a possibilidade de interferir nas comunicações, ainda que cifradas, ligar remotamente a câmara e/ou o microfone, por exemplo. No fundo aceder à informação a partir da fonte, tenha ou não existido comunicação entre o suspeito e terceiros. Desta feita existem situações problemáticas que urge acautelar com a utilização destes recursos colocados à disposição da investigação criminal.

A luta contra a criminalidade, independentemente da sua natureza, é um trabalho contínuo que requer técnicas ajustadas às novas realidades tecnológicas, disso não temos dúvidas, como se exige que a legislação permita o uso destas na recolha de prova e imputação da responsabilidade jurídico-penal. Cabe ao Direito não deixar de fora este acompanhamento pois se tal acontecer os criminosos sentir-se-ão confortáveis nos seus modos de atuação e os investigadores criminais poderão estar a recorrer a métodos de prova proibidos inquinando os princípios mais elementares do Estado de Direito, no que ao Processo Penal diz respeito. O Estado tem por obrigação proteger, com o seu *ius imperium*, os seus cidadãos e aplicar a justiça contra aqueles que efetivamente prevaricam e praticam atos ilícitos, que colocam em causa os *bens jurídicos*, tal como o da confiança nos sistemas informáticos e nas redes de comunicações, essencial à manutenção de uma sociedade moderna[7].

[7] Como diz Jock Young, *"o papel do Estado do bem-estar social é assimilar os desviantes, integrando-os no corpo da sociedade"*. Jock Young, *A sociedade excludente: exclusão social, criminalidade e diferença na sociedade recente*, Rio de Janeiro: Revan, 2002, *Cit.*, p. 21.

2. Delimitação do tema

§1. O tema da prova, em sede penal, está intimamente ligado à *presunção de inocência* dos arguidos. São as provas vertidas na acusação e dadas como provadas em julgamento (*princípio da imediação*) que aferem do grau de culpa e responsabilidade criminal, pois que sem provas ou no caso de dúvida acerca da intervenção do arguido (*in dúbio pro reo*) cuminará na sua absolvição.

O método de obtenção de prova utilizado é igualmente essencial para a validade daquela, de modo que possa ser usada em tribunal e não vá inquinar a finalidade do processo penal, isto é, a *descoberta da verdade material*[8].

A figura do agente encoberto, a par de outros métodos de obtenção de prova, acarreta consigo diversos problemas que poderão consubstanciar: (1) proibições de prova, caso não sejam cumpridos os formalismos inerentes à sua atuação ou extravasem a atuação deste[9], em obediência às normas legais e princípios constitucionais; (2) violar princípios consagrados constitucionalmente como as comunicações e a correspondência; (3) afetar de grosso modo Direitos, Liberdades e Garantias dos cidadãos, como o direito à livre circulação, à reserva e intimidade da vida privada, entre outros.

§2. Com a proliferação da internet e dos problemas que surgiram e o Direito tinha que dar resposta, o legislador nacional viu-se obrigado a adaptar o direito interno à Legislação que então vigorava sobre a Criminalidade Informática. Eis que surgiu a Lei do Cibercrime (LC), Lei n.º 109/2009, de 15 de setembro, aquando da ratificação da Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001.

A Convenção não detém nenhuma norma relativamente às ações encobertas por meios tecnológicos. A estatuição de uma regra jurídica pelo legislador nacional, diga-se em abono da verdade, não é inovadora do ponto de vista sistemático e teleológico, indo além do previsto nos ins-

[8] Maria João Antunes, *Direito Processual Penal*, Almedina, 2017, pp. 23-27.

[9] Manuel da Costa Andrade, *Sobre as proibições de prova em processo penal*, Coimbra, Coimbra Editora, 1.ª Edição (Reimpressão), 2013, pp. 209 a 233; Eduardo da Maia Costa, «Agente provocador – validade das provas», *Revista do Ministério Público*, Ano 21, n.º 81, (janeiro-março de 2000), pp. 155 a 174, entre outros.

trumentos legislativos internacionais que adotou[10]. Procedeu, no art. 19.º da Lei do Cibercrime, à aplicação *mutatis mutandis* do regime das ações encobertas, Lei n.º 101/2001, de 25 de agosto. Alargou-se ao Regime Jurídico do Agente Encoberto o cátalogo de crimes, sendo agora aplicável quanto aos crimes previstos na Lei do Cibercrime ou cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes. Bem como à burla qualificada, à burla informática e nas comunicações, à discriminação racial, religiosa ou sexual, às infrações económico-financeiras, e, ainda, aos crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

§3. A inovação legislativa surge quando se menciona que sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações. Deste modo, resultou inequivocamente uma confusão de conceitos diferentes numa só situação, dito de outro modo, prevê-se a utilização ativa de um agente encoberto digital e a interceções de comunicações em dispositivos informáticos numa única situação. Duas realidades distintas e que são incompatíveis quer do ponto de vista dos métodos de obtenção de prova, quer nos distintos regimes processuais em vigor, mormente do controle da legalidade, como veremos adiante.

2.1. Colocação do problema

§1. Das diversas questões inicialmente prognósticadas decidimos condensá-las em quatro quesitos, seguindo os ensinamentos de Karl Larenz, quando nos refere que o problema deve ser abordado a "*partir dos mais diversos ângulos e que traga à colação todos os pontos de vista – tanto os obtidos a partir da lei como os de natureza extrajurídica*"[11]. Cientes deste aspeto

[10] Para além da Ciberconvenção foi transposta para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação.

[11] Karl Larenz, *Ob. Cit.*, p. 201.

tomamos em consideração todos os elementos imprescindíveis para uma investigação sólida e concreta com o desígnio de obter respostas concretas. Condensamos os problemas para não existir uma dispersão inexaurível de pensamentos paralelos que poderiam tornar a investigação confusa e sem qualidade científica. Tivemos, assim, por fito apenas abordar as questões mais prementes e debatê-las profusamente com o intuito de almejarmos respostas credíveis.

§2. *Primum*, impõe-se, desde logo, questionar se a lei positiva permite efetivamente a ação do agente encoberto nas redes digitais. Ou dito de outro modo, se o art. 19.º da LC que remete para o regime do agente encoberto (lei n.º 101/2001, de 25 de agosto, na sua redação atual pela lei n.º 79/2021, de 24 de novembro), com o incremento que sendo necessário o recurso a meios e dispositivos informáticos observar-se-á, naquilo que for aplicável, as regras previstas para a interceção de comunicações, será, de *per si*, suficiente para levar a cabo uma ação de investigação encoberta na internet.

§3. *Secundum*, se os agentes de investigação poderão enviar *benware*[12] para um sistema informático de um suspeito, com o intuito de verificarem, sem ser detetados, que conteúdos o suspeito detém no seu computador, *smartphone* ou outro equipamento. Pretende-se obter a informação na fonte, por diversos motivos, não apenas quando efetivamente exista uma comunicação, mas também toda a informação que exista nesse ou nesses dispositivos informáticos. Tal diligência é fulcral, por um lado, em casos de abuso sexual de menores, designado na gíria popular por pedofilia, por ser notório que esta partilha de imagens apenas acontece em circuitos muito restritos e sempre com base na confiança do interlocutor e por troca de novas imagens. Por outro, será importante porquanto

[12] *Benware*, por oposição a *malware* (*software* malicioso), é um *software* benigno, benevolente. Achamos que a expressão a utilizar é a mais correta que *malware* pois não tem como finalidade provocar algum mal ao utilizador ou no dispositivo informático, mas tão somente conseguir aceder ao mesmo e visualizar o que ali se encontra alojado. Definição retirada do Dicionário AZDictionary, acessível em https://www.azdictionary.com/urban-dictionary/definition/benware [*acedido em 25 de janeiro de 2015*].

as conversações entre cibercriminosos se fazem através de redes *peer-to-peer*, tais como aplicações informáticas de envio/receção de mensagens, ficheiros, vídeos e audio, por exemplo, de forma encriptada.

A este tipo de ação denominaremos de ação técnica encoberta, porquanto a mesma não necessita de um agente físico encoberto no sistema informático uma vez que todo o processo se realiza com a utilização de *software* específico que batizamos de *benware*.

O *benware* seria igualmente utilizado, porque a tecnologia assim o permite, para ativar a câmara de vídeo e/ou o microfone, sem que o alvo da investigação de apercebesse de algo, podendo ser importante esta ação em casos de corrupção, por exemplo, onde a prova é de difícil obtenção. Esatremos, desta forma, no âmbito da utilização de meios especiais e técnicos de investigação criminal.

A crescente forma de encriptação de conteúdos, no que toca à transmissão de dados, mormente pelo uso da *darkweb*, em especial as redes TOR, não será um motivo de valor acrescido para a utilização do agente encoberto digital na descoberta e identificação dos criminosos? É que para além da encriptação há enormes recursos informáticos de anonimização e no mundo *obscuro* da internet há uma criminalidade organizada que se dedica não só a casos de pedofilia, mas também à venda de muitos produtos ilícitos, tais como armas, produtos estupefacientes, documentos falsificados e tantos outros que não são consentidos numa sociedade onde imperam valores éticos, morais e legais.

§4. *Tertium*, se a criação de perfis falsos automatizados[13], que conseguem coligir, processar e trocar informação através de determinados parâmetros, algoritmos previamente estabelecidos, desde que supervi-

[13] A este respeito, que abordaremos posteriormente, chamamos à colação a figura da menina virtual, apelidada de *Sweetie*, criada pela ONG *Terre des Hommes*, que no espaço de dez semanas logrou identificar mais de mil suspeitos de abuso sexual de menores, pertencentes a 71 países. Da informação veiculada em diferentes órgãos de comunicação social remetemos para os mais importantes: o site do projeto https://www.terredeshommes.nl/en/sweetie-face-webcam-child-sex-tourism, bem como http://www.slashgear.com/sweetie-virtual-child-takes-down-1000-pedophiles-in-10-weeks-06304515/ e, ainda, http://abcnews.go.com/WNT/video/meet-sweetie-virtual-girl-identified-1000-pedophiles-world-20797023 [*acedidos em 25 de janeiro de 2015*].

sionados pela autoridade judiciária competente, podem servir de prova, afastando, assim, a figura do agente provocador. É muito discutido na jurisprudência e na doutrina qual a fronteira entre o agente encoberto e o agente provocador, sabendo-se que ambas as figuras vivem "paredes meias", levando a que, por vezes, alguma da prova recolhida venha a ser considera nula e não possa ser utilizada na incriminação dos arguidos.

§5. *Quartum*, se a utilização de "balizas" GPS, sistemas que conseguem detetar a posição exata de um alvo através de GPS, é permitida pela atual lei do agente encoberto.

O recurso à posição GPS é de extrema importância porquanto consegue-se à distância monitorizar um indivíduo sem que este se aperceba que está a ser "seguido". Tal diligência poderá produzir efeitos úteis para a investigação e encetar outras diligências que conduzirão à recolha de prova, que de outra forma seria impossível de obter.

§6. *Quintum*, acresce a esta situação a utilização, cada vez mais em voga, de dispositivos de captação de imagem e som (*voz off*), quer através de *drones*[14] *quer através dos próprios dispositivos informáticos, nos quais se destaca o smartphone* do alvo a ser vigiado, por introdução de *software* específico neste aparelho, como mencionado anteriormente, quer através de GPS que possuem acoplados cartões de telefone, que para além das coordenadas geográficas permitem ouvir o ambiente que o rodeia.

§7. Deverão estas possibilidades tecnológicos estarem regulamentadas por forma a que efetivamente as imagens e sons captados possam servir de prova em sede de julgamento no âmbito penal? Não podemos olvidar que na captação destas imagens podem ser violados diversos preceitos, mormente a intimidade e a reserva privada de cidadãos que nada têm a ver com a situação, o direito à imagem das pessoas visadas, para além de que pode constituir um crime, tipificado no art. 190.º do CP, caso não se aplique o regime da Lei n.º 5/2002, de 11 de janeiro, por exemplo.

[14] *Drone* traduzido literalmente do inglês significa "zangão". Designa, assim, qualquer tipo de aeronave não tripulada, mas comandada á distância que capta, grava e transmite imagens em tempo real ou em diferido.

2.2. Estrutura e modo de abordagem do problema

§1. O nosso trabalho assentará em dois pilares fulcrais. Na primeira parte, a que denominamos de **Parte Geral**, analisamos o paradigma do agente encoberto. Abordaremos as situações que contendem com o agente encoberto e que têm sido alvo de apreciação pelos tribunais superiores, tais como o agente provocador, homens de confiança, conhecimentos fortuitos, etc. Na **Parte Especial** escalpelizamos o recurso ao agente encoberto nas redes de informação e comunicação, a que denominaremos de *agente encoberto digital*. Aproveitamos, deste modo, para fazer a ponte entre estas duas realidades sem paralelo e verificar se existe ou não alguma incongruência legislativa na adoção do mesmo regime jurídico de obtenção de prova do agente encoberto em situações distintas: a analógica e a digital.

§2. Subdividimos a Parte Geral em duas. Por um lado, a figura do agente encoberto, enquanto ferramenta essencial de obtenção de prova e meio de descoberta da verdade material e, por outro, a problemática da cibercriminalidade e as vicissitudes da sua investigação. Qual o escopo do agente encoberto, nos termos da Lei n.º 1010/2001 e da própria doutrina?

Donde, após uma breve resenha histórica, dissecamos o atual regime do agente encoberto tendo como "linha do horizonte" a sua aplicabilidade às investigações realizadas através de meios informáticos. E como o meio de atuação do agente encoberto é bem destinto da realidade física, por se tratar do ciberespaço, debruçamo-nos sobre a aplicabilidade às investigações *online*.

Concorrem diversos fatores no tangente às investigações *online*. A desterritorialidade[15] leva a que investigações ocorram em países terceiros sem que as entidades desses países tenham conhecimento de tais investigações, não existindo a possibilidade de negar ou autorizar tais medidas

[15] Daniel Freire e Almeida defende a criação de um Tribunal Internacional para a Internet, para dirimir conflitos cíveis e comerciais. Advoga que "*[o] sistema no qual funciona a Internet é indiferente quanto à localização física dos computadores, e não há ligação necessária e precisa entre um endereço de Internet e uma jurisdição física*", In *Um Tribunal Internacional para a Internet*, Almedina, Coimbra, 2015, p. 152.

de ingerência na sua soberania[16]. Donde, analisaremos também as formas de anonimização, com recurso a redes TOR, a VPN's, etc, e o cruzamento de informação que se pode obter através de pesquisas OSINT[17].

[16] Os arts. 82.º a 86.º do Tratado sobre o Funcionamento da União Europeia (TFUE) tratam sobre a cooperação judiciária em matéria penal, com especial ênfase no princípio do reconhecimento mútuo de sentenças e decisões judiciais. Inclui matéria penal sempre que se afigure indispensável para assegurar a execução eficaz de uma política da União. É com a criação da Eurojust (art. 85.º do TFUE) que existe uma aproximação entre os Estados-Membros em matéria de cooperação, podendo esta entidade proceder: "*a) A abertura de investigações criminais e a proposta de instauração de acções penais conduzidas pelas autoridades nacionais competentes, em especial as relativas a infracções lesivas dos interesses financeiros da União;*
b) A coordenação das investigações e acções penais referidas na alínea a);
c) O reforço da cooperação judiciária, inclusive mediante a resolução de conflitos de jurisdição e uma estreita cooperação com a Rede Judiciária Europeia."
Em momento algum é prevista a ingerência de um Estado noutro Estado, mas apenas cooperação a nível europeu, referindo o n.º 2 do art. 85.º que "*os actos oficiais do procedimento judicial são executados pelos agentes nacionais competentes*."
As investigações através da internet poderão levar a que se investigue uma rede criminosa, com origem em diversos países, mas a detenção desses membros apenas poderá ocorrer se os mesmos estiverem na circunscrição jurídico-territorial competente de quem investiga. De outro modo, para além de não se criarem conflitos graves de ingerência em vários países, as detenções apenas poderão ocorrer com a comunicação às autoridades competentes desse país, com a indicação de todos os elementos apurados e relevantes para o caso. Como se sabe, a prova digital é volátil e num ápice os elementos investigados, se não forem prontamente corroborados pelas entidades desse país, poderão deixar de existir.
Ainda no que concerne à desterritorialidade sucede que um criminoso possa provocar danos em vítimas de vários países com a mesma e única ação ilícita, por exemplo o envio de *malware* para diversos computadores, infetando vários milhares de computadores e lesando várias vítimas através do pagamento de resgate dos dados que ali se encontravam guardados. Qual a competência judicial para efetivamente investigar e julgar este indivíduo? O local onde reside habitualmente? Onde surgiu a notícia do primeiro facto criminoso? Todos os países são competentes para o julgar?
Estas e outras *vexata quaestiones* são cada vez mais prementes quando falamos num tipo de criminalidade que não conhece fronteiras e quando a sua forma de investigar tem que ser cada vez mais rebuscada, inteligente e requer rapidez de ação, pois os criminosos também se adaptam e usam estratégias que os tornam "invisíveis".

[17] OSINT – *Open source intelligence*. Usaremos a presente sigla ou a expressão "pesquisa em fontes abertas" na internet.

§3. Numa segunda parte, a que chamamos **Parte Especial**, lançamos mão especificamente na análise do agente encoberto nas tecnologias de informação e comunicação.

Não poderíamos encetar esta parte – o agente encoberto em ambientes digitais – sem analisar o estado da arte e abordar os ordenamentos jurídicos que maior influência têm sobre o nosso sistema jurídico, o alemão e o italiano. Convocamos, neste sistema comparativo, o ordenamento espanhol por força das recentes alterações legislativas, onde se introduziu no CPP a investigação com recurso ao agente encoberto digital.

A investigação prossegue sobre o uso de diversas ferramentas forenses que colocadas na mão de um agente encoberto podem recolher provas irrefutáveis da prática de vários ilícitos criminais praticados na internet. Desde logo o recurso a *software* específico para visualizar conteúdos que se encontrem alojados nos sistemas computacionais dos suspeitos. A utilização de drones e de balizas GPS dissimuladamente na prevenção e investigação de ilícitos criminais. E, de não somenos importância, o recurso a mecanismos virtuais para investigação de crimes informáticos. Até que ponto o automatismo substitui o agente encoberto ou tratar-se-á da mesma figura, mas cujo objeto é diferente?

Posteriormente iremos analisar casos verídicos em que a figura do agente encoberto nas redes informáticas foi fulcral para a descoberta dos meliantes e lograr uma investigação profícua, com a detenção dos mesmos. Abordaremos o *caso Silk Road*, que teve a sua génese e desfecho nos Estados Unidos da América. A nível europeu analisaremos o *caso Sweetie* e a sua admissibilidade jurídica no ordenamento nacional. Concomitantemente também analisaremos a nível europeu a recente ação coordenada pela Europol, em julho de 2017, cuja operação *Bayonet* desmantelou dois dos maiores mercados negros da *Darkweb*.

O primeiro caso refere-se a um mercado *obscuro* que vendia todo o tipo de armas, de drogas, de cartões de crédito falsificados, documentos contrafeitos, etc, com recurso à rede TOR na *darkweb*; o segundo reporta-se a uma menina virtual que atraiu as atenções de diversos predadores sexuais, interessados em relacionamentos sexuais com menores, levando à identificação e detenção de vários pedófilos em muitos países, alguns deles fora do perímetro europeu. Como mencionado a operação *Bayonet* foi realizada tendo como pano de fundo a cooperação judiciária operada

com diversas agências de investigação criminal de vários países. Nesta operação decorreu o desmantelamento de dois mercados negros, localizados na internet obscura, *darkweb*. Um destes mercados foi investigado pelo FBI e o outro pela Polícia Nacional Holandesa, com recurso a agentes encobertos digitais. A Europol foi a coordenadora da operação, uma vez que a investigação ocorreu em simultâneo em vários países e envolveu diversas instituições de investigação criminal.

Por último, dedicaremos um capítulo às conclusões, almejando humildemente uma resposta para as quatro questões que formulamos *supra*. Antes, porém, deixamos uma visão sobre o futuro, analisando a evolução tecnológica que nos espera, em especial sobre a internet das coisas (IoT), bem como, com carácter construtivo, a urgência de novas leis processuais penais no tocante a esta matéria do agente encoberto na internet.

ÍNDICE

PARTE ESPECIAL – O AGENTE ENCOBERTO VS AS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO