Instituto Superior de Ciências Policiais e Segurança Interna

As novas tecnologias e a investigação criminal:

a obtenção da prova

Autor: Comissário Maria de Fátima Magalhães da Rocha

Artigo de estudo teórico

Lisboa, 12 de Julho de 2019

As novas tecnologias e a investigação criminal:

a obtenção da prova

Trabalho Individual Final

III Curso de Comando e Direção Policial

Maria de Fátima Magalhães da Rocha
Comissário

Resumo

A evolução tecnológica trouxe consigo muitas vantagens, facilitando a vida em sociedade sob os mais diversos aspectos. Contudo, essa evolução foi transversal às mais distintas áreas, não ficando de fora o fenómeno criminógeno, que viu na Internet um portal aberto para a prática de crimes e transações ilícitas sem qualquer traço de vestígio. Numa luta desigual as polícias apelam, também, à tecnologia para combater uma criminalidade cada vez mais cibernética. Mas deparam-se com uma legislação que não está ainda totalmente preparada para esta nova realidade e cujo escopo é a proteção de direitos, liberdades e garantias, nomeadamente a proteção do direito à privacidade. O auxílio que é solicitado pelo Ministério Público na investigação criminal e na recolha de provas indiciárias é, frequentemente, confinado por uma limitação à atuação policial, nomeadamente no que diz respeito à obtenção da prova. Sujeitos a estas restrições, a linha entre o meio de prova permitido e o meio de prova proibido torna-se muito ténue conduzindo, não raras vezes, a provas obtidas ilegalmente. Esta problemática prende-se concretamente com o meio de obtenção de prova no meio digital e a sua volatilidade.

Palavras-chave: Investigação criminal, órgão de polícia criminal, meio oculto de obtenção de prova, novas tecnologias.

Abstract

The evolution of technology brought lots of benefits, facilitating life in society in the most diverse aspects. However, that evolution was transverse to other diferent fields, including the criminological phenomenon, which saw in Internet an open gate to commit crimes anda illicit operations without being detected. In an unequal struggle polices also they appeal to technology to fight cyber crime. But they are confronted with a law that it isn't totally prepared to this new reality and whose scope is the protection of rights, freedoms and garantes, in particularly the protection of right to privacy. The aid requested by the Public Prosecutor's Office in the criminal investigation and in the collection of evidence is often confined by a limitation of policie action particularly with regard to obtaining evidence. Under these restrictions, the line between the permitted means of proof and the prohibited means of proof becomes very tenuous leading to evidence obtained illegally. This problema is specifically related to the means of obtaining evidence in the digital environment and its volatility.

Keywords: Criminal investigation, criminal police agency, news technologies, secrets methods of evidence.

Índice:

Introdução

As últimas décadas têm sido marcadas por um intenso desenvolvimento tecnológico. Não só as fronteiras se tornaram cada vez mais ténues dando forma à aldeia global da qual fazemos parte, como também as sociedades têm sofrido mudanças a um nível cultural e criminal. Todas estas alterações refletem-se invariavelmente no ordenamento jurídico que face a um novo tipo de criminalidade deve adaptar-se e reajustar-se de forma a controlar novos fenómenos criminógenos. Esta criminalidade tem as suas fundações em operações virtuais, indivíduos e grupos que se desenvolvem e organizam silenciosamente, com um carácter transnacional e sofisticado, minando economias e estados de direito democráticos. Há, por parte dos estados, uma preocupação crescente com este tipo de criminalidade que se revela cada vez mais grave ameaçando a própria democracia. Impera, por isso, a necessidade de reformular normativos legais para criar formas eficazes de combater esta "criminalidade organizada e internacionalizada" (Susano, 2009, p.12).

Assistimos nos últimos anos a alterações ao Código de Processo Penal (as quais ficaram um pouco aquém das expectativas de quem esperava algo mais de uma alteração que se considerou e previa que fosse mais profunda), assim como à criação de uma lei que veio mudar o tratamento processual penal das comunicações electrónicas – a Lei nº 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre o Cibercrime do Conselho da Europa. Resta saber se essas alterações vieram trazer algum (desas)sossego a uma sociedade que clama por mais segurança e justiça.

No ordenamento jurídico português a adoção de medidas de investigação que colidam com direitos, liberdades e garantias dos cidadãos são de caráter excepcional e revelam-se de alguma cautela na sua utilização, cabendo à autoridade judiciária a decisão da autorização do seu uso. Referimo-nos a meios mais invasivos da privacidade do indivíduo, como a utilização das escutas telefónicas, da vigilância da correspondência electrónica e da localização celular, sendo que são as únicas medidas (ainda) autorizadas na investigação criminal. Estes meios de obtenção de prova são autorizados mediante despacho fundamentado da autoridade judiciária de que, perante o *periculum in mora*, aquela medida é a única disponível perante a necessidade da investigação, esgotadas que foram todas as outras menos invasivas da privacidade do cidadão.

Num mundo cada vez mais virtual, o combate ao cibercrime torna-se desigual. Enquanto que existem organizações criminosas muito bem dotadas de aparelhos tecnológicos e com membros integrantes bastante conhecedores do ambiente digital, as polícias continuam enredadas em novelos jurídicos de limitações à sua atuação contra este tipo de criminalidade. E é sobre este ponto que pretendemos chamar a atenção para a importância do trabalho investigatório das polícias, que é a possibilidade do processo penal recuar na proteção de determinados direitos quando esteja em causa a descoberta da verdade material de crimes relacionados com terrorismo, criminalidade muito grave e organizada. Esta é uma problemática que iremos explorar ao longo do presente estudo: Deverá o direito processual penal recuar nos seus dogmas quando estiver em causa aquele tipo de criminalidade que, virtualmente e como um fantasma, assombra a segurança da sociedade e a própria segurança de um estado de direito democrático? É verdade que o *ius cogens* impõe o cumprimento de normativos inderrogáveis, mas pretende-se tão somente criar meios investigatórios de carácter excecional que agilizem a tarefa investigatória das polícias.

Em bom rigor, pretendemos fazer uma apresentação no nosso estudo sobre a exploração do direito processual penal e legislação avulsa relacionada com a atuação policial no que à investigação do cibercrime diga respeito. Esta incursão teórica trará a lume as dificuldades que existem durante uma investigação criminal em que esteja em causa não só os crimes praticados através do espaço virtual, mas também o uso de instrumentos tecnológicos capazes de rastrear e monitorizar indivíduos suspeitos da prática de terrorismo, crimes graves e criminalidade organizada. O objectivo será o de demonstrar que uma abertura na proibição imposta ao uso de meios (ocultos) de obtenção de prova, cujo carácter intrusivo nos direitos constitucionalmente consagrados impossibilita a atuação policial, potenciará os resultados da investigação, defendendo a visão de que perante uma "crescente evolução tecnológica, em que os agentes do crime se munem de artifícios sofisticados para despistar os investigadores, também se impõe que a estes sejam concedidos os meios que assegurem a eficácia da investigação" (Susano, 2009, p. 34).

Estado de Arte

Hipóteses Teóricas:

No sentido de conseguirmos dar uma resposta à problemática levantada e de vermos satisfeitos o nosso objectivo, somos levados a colocar as seguintes hipóteses conceptuais: 1) Corroborar ou não corroborar a admissibilidade da abertura de excepcionalidade do uso de outros meios de obtenção de prova para além dos elencados no art. 187.º e seguintes, no art. 251.º e seguintes do Código de Processo Penal; 2) Corroborar ou não corroborar a admissibilidade da abertura de excepcionalidade do uso de outros meios de obtenção de prova para além dos elencados no art. 15.º e seguintes da Lei n.º 105/2009 de 15 de setembro; 3) Corroborar ou não corroborar que a acentuada criminalidade organizada, transnacional, terrorismo e cibercrime são ameaças que justificam a necessidade dessa admissibilidade excepcional.

Contextualização Teórica:

Os meios ocultos de obtenção de prova têm também sido alvo de discussão muito acesa nas últimas décadas, derivado supostamente das alterações sociais que se têm vivido e que se refletem em comportamentos desviantes cada vez mais sofisticados e virtuais. E este tem sido um assunto largamente debatido devido à preocupação com o cibercrime que encontra na Internet um terreno fértil e facilitador para os seus negócios ilícitos.

Para as polícias o trabalho não se revela fácil uma vez que a prova digital é uma prova fungível que rapidamente se desvanece e que facilmente é apagada sem deixar qualquer rasto da existência do crime cometido. Falamos em polícias por se tratarem de órgãos de polícia criminal (OPC) cujas competências são idênticas, uma vez que no que ao processo penal diz respeito, "a posição jurídico-institucional dos corpos orgânicos designados como Polícia Judiciária, Polícia de Segurança Pública e Guarda Nacional Republicana [é] idêntica" (Mesquita, 2010, p. 382).

E a função da polícia surge-nos consagrada na Constituição da República Portuguesa (CRP), no seu art. 272.º, onde está vertida a ideia de defesa da legalidade democrática assim como o respeito pelo cumprimento das medidas de polícia no estritamente necessário e com a prossecução do princípio da legalidade e do respeito pelos direitos, liberdades e garantias dos cidadãos.

Essa concepção de polícia e de tutela de direitos, liberdades e garantias, também está plasmada na Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna (LSI) – cujas últimas alterações foram introduzidas pela Lei n.º 21/2019, de 25 de fevereiro – , onde o legislador reafirma essa função das forças e serviços de segurança de subordinação ao princípio da legalidade bem como de manutenção da ordem, tranquilidade e segurança públicas, e proteção contra ameaças que possam fazer perigar a segurança interna, sobressaindo no n.º 3 do seu art. 1.º a relevância dessa proteção em especial contra "o terrorismo, a criminalidade violenta ou altamente organizada".

Já a Lei n.º 49/2008, de 27 de Agosto que aprova a Lei da Organização e Investigação Criminal (LOIC) especifica quais são os órgãos de polícia criminal de competência genérica, que é o que releva para o nosso estudo – Polícia judiciária, Polícia de Segurança Pública e Guarda Nacional Republicana, indo um pouco ao encontro da posição já defendida por Mesquita e por nós anteriormente citado. A Lei n.º 96/2017, de 23 de agosto, que aprova a Lei de Política Criminal para o Biénio de 2017-2019, realça logo no seu art.º 2.º a prioridade de crimes como o terrorismo, a criminalidade violenta e organizada e a cibercriminalidade. O legislador está ciente de que este fenómeno de crimes, como o mesmo indica no art. 2.º, desta Lei de Política Criminal, é um risco para a segurança da sociedade e uma ameaça às pedras basilares de um Estado de direito democrático: segurança, justiça, economia, liberdade; e o legislador torna não só a prevenção como também a investigação (art. 3.º da mesma Lei) e a luta contra este tipo de crimes uma prioridade nas atribuições às autoridades judiciais e aos órgãos de polícia criminal, como elementos coadjuvantes que são do MP.

Com vista a criar instrumentos de defesa contra estas novas ameaças que surgem fruto da globalização, havia sido criada anteriormente a Lei n.º 5/2002, de 11 de janeiro, que estabeleceu um conjunto de medidas de combate à criminalidade organizada e económico-financeira. Neste diploma pode ler-se um catálogo de crimes que, pela sua gravidade, mereceram da parte do legislador a criação de "um regime especial de recolha de prova", como o mesmo indica no n.º 1 do art. 1.º desta Lei. O legislador faz ainda a remissão para a Lei n.º 109/2009 de 15 de setembro – Lei do Cibercrime – ou seja, a recolha de prova quando se verificarem os pressupostos inscritos no n.º 1, al. *m)* e n.º 4, ambos do art. 1.º, da Lei n.º 5/2002 de 11 de janeiro. Ora, esta remissão que o legislador faz para a Lei do Cibercrime já fora plasmada naquela lei numa fase muito posterior à redação original da Lei n.º 5/2002, de 11 de Janeiro. Tratou-se da sexta alteração à Lei n.º 5/2002, de 11 de janeiro, introduzida pela Lei n.º 30/2017 de 30 de maio, e em concreto no seu art. 2.º. E

esta remissão já prevê uma excepcionalidade da norma no que diz respeito à recolha de prova, salvaguardando, é certo, determinados pressupostos, elencados no art. 6.º da mesma Lei, assim como os que vêm previstos no art. 188.º do CPP. A recolha de prova, prevista no art. 6.º da Lei n.º 5/2002, de 11 de janeiro, prevê a gravação de voz e imagem, através de qualquer meio, sem a necessidade do consentimento do visado, havendo lugar apenas à autorização ou ordem prévia da autoridade judiciária.

Na verdade, o legislador considera que a gravidade dos crimes elencados nesta lei ameaçam de tal forma a segurança, não só dos cidadãos, como do próprio Estado, e que o recurso às novas tecnologias por parte dos agentes do crime são cada vez mais inovadoras no sentido de ludibriar as autoridades, que deve conceder-se a estas os meios investigatórios necessários que assegurem a eficácia e o sucesso da investigação, sem perder de rumo, contudo, princípios garantísticos como o princípio da proporcionalidade (nas suas três vertentes: necessidade, adequação e da proporcionalidade em sentido estrito) em conjunto com o princípio da ponderação face o caso em concreto.

Em bom rigor, fazendo novamente uma incursão pela CRP – o princípio da legalidade democrática que nos surge no art. 3.º, n.º 2 da CRP – temos a efetiva proteção contra a ingerência na correspondência e nas comunicações o que está invariavelmente relacionado com a proteção da intimidade da vida privada, e da própria dignidade da pessoa humana – princípio este plasmado no art.º 1.º da CRP. Em particular, o art. 34.º, n.º 4, da CRP estabelece assertivamente a proibição dessa intrusão pelas autoridades "na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal". Aqui, a *Lex Mater* remete-nos para o CPP onde podemos encontrar essa admissibilidade da intrusão na correspondência e nas comunicações dos cidadãos nos seus arts. 179.º, 187.º, 189.º e 252.º-A, medidas estas de carácter excepcional e destinadas somente aos crimes legalmente sistematizados.

O catálogo de crimes ínsito no art. 187.º daquele diploma legal descreve quais os ilícitos criminais em que é admissível a ingerência na correspondência e nas comunicações.

A nível europeu, a cibercriminalidade representou uma preocupação transversal a todos os Estados-membros pelo que emitiu, através da Convenção do Conselho da Europa regras que deveriam ser aplicadas no ordenamento jurídico português. Com a publicação da Lei n.º 109/2009, de 15 de setembro, admitiu-se uma nova realidade na obtenção da prova: a recolha de prova em suporte electrónico. Passa, assim, o correio electrónico bem como outros registos de comunicações de natureza semelhante a ter um tratamento

específico, aplicando-se concomitantemente o regime da apreensão de correspondência previsto no CPP, tal como referem os arts. 17.º e 18.º da Lei do Cibercrime.

A Proposta de Lei n.º 289/X/4.ª, na sua Exposição de Motivos, infere largamente sobre essa remissão para o CPP, justificando que "torna-se necessário abranger os crimes informáticos em geral, bem como aqueles cometidos por via de computadores, assim se motivando a criação de norma especial. Esta norma adopta em geral as regras do Código de Processo Penal, que é adaptado em função da especificidade dos crimes a que por via desta nova lei, é aplicável" (P.L. n.º 289/X/4.ª) realçando ainda que o regime de buscas e apreensões que tem acolhimento no CPP foi adaptado à investigação da cibercriminalidade, num claro ajuste do regime existente ao novo fenómeno criminógeno. Na verdade, a referida Proposta "abre" o leque de crimes que seria expectável que fosse restrito, a "crimes informáticos em geral", surgindo na Lei do Cibercrime duas situações: 1) cibercrimes; 2) crimes informáticos em geral.

A criação da Lei do Cibercrime possibilitou a concentração de todo o procedimento processual relativamente a cibercrimes, além dos crimes cometidos através de um sistema informático e, como já foi mencionado anteriormente, também àqueles crimes sobre os quais recaia a necessidade de recolha de prova electrónica, tal como vem explícito no art. 11.º desta Lei. De referir que ao invés de se proceder à alteração de diversas leis no sentido de nelas incluir os crimes relacionados com o espaço virtual, procedeu-se à criação da Lei do Cibercrime onde estão condensadas e sistematizadas todas as normas que dizem respeito à cibercriminalidade. Com este diploma legal e as suas medidas processuais, assiste-se a uma nova realidade no que diz respeito à obtenção da prova e à sua recolha.

Somos de referir que existem posições contraditórias quanto à utilização de uma legislação avulsa para categorizar crimes que deveriam estar incluídos no Código de Processo Penal, mais concretamente no Livro III (a prova), abrindo possivelmente um novo capítulo, por exemplo, a "prova electrónica" (Mesquita, 2010, p. 101), posição esta com a qual concordamos.

Apesar deste paradoxo legislativo, verificamos que à semelhança dos meios de obtenção de prova inscritos no CPP, também a Lei do Cibercrime adopta um sistema muito idêntico, levando à compressão de direitos constitucionalmente consagrados. Cabe ao juiz a decisão da junção de determinados dados ou documentos informáticos apreendidos, consoante sejam ou não pertinentes para o processo, mesmo que o seu conteúdo seja susceptível de revelar dados pessoais ou íntimos capazes de colocar em causa a intimidade

e a privacidade do titular ou de terceiro, conforme faz menção o n.º 3, do art. 16, da Lei do Cibercrime.

A compressão de direitos consagrados no caso da cibercriminalidade passa pelo espaço cibernético e por toda a informação e documentação que esteja armazenada em espaço digital, revelando-se de alguma complexidade, para a autoridade judiciária e para os órgãos de polícia criminal, fazer aquela separação no momento da apreensão dos documentos, não só daquilo que se revela ou não fulcral para o caso em concreto, como também o que é ou não parte da privacidade do visado ou de terceiro. Muito embora o direito à autodeterminação informacional seja cada vez mais debatido como um direito a ser defendido a par do direito à privacidade, cremos que "não se trata, naturalmente, de um direito tutelado de forma ilimitada: como ser social por natureza, o indivíduo tem de suportar limitações ao seu direito de autodeterminação sobre a informação em nome de interesses prevalecentes da comunidade" (Gossel, 1992, p. 432).

Ademais, a possibilidade de perda da informação virtual aquando da sua recolha do local onde se encontra armazenada, que é algo que está sempre iminente de acontecer, é outra razão para que, no caso de recolha de prova virtual de natureza íntima ou privada, caiba ao juiz a decisão da junção ao processo. Nisto reside a livre apreciação da prova por parte do juiz e que vem consignada no art. 127.º do CPP. Por exemplo, em casos de pornografia infantil, pedofilia, tráfico de seres humanos, tráfico sexual, ou seja, criminalidade grave ou organizada, o juiz pode decidir que mesmo a informação de índole privada pode conter informação pertinente para o apuramento da verdade e ordenar a sua junção ao processo.

Perante uma era em que temos um espaço virtual, normativamente desregulado, de fácil acesso e navegação, onde se pode aceder a outros níveis de informação mais obscura e de natureza criminógena – a *Dark Web* – , locais onde se escolhem vítimas de forma indiscriminada e sem qualquer escrúpulos, encomendando-se e cometendo-se crimes, é necessário analisar, repensar e refletir sobre esta limitação de direitos, liberdades e garantias que tanto se invoca, quando está em causa o cometimento de crimes de tão grande gravidade e cuja evolução tecnológica criminosa se prevê que aumente. E decorrente dessa proibição de supressão de direitos constitucionalmente protegidos cremos que reside uma limitação à investigação criminal da cibercriminalidade. Deste modo, podemos afirmar que a sociedade da informação é, também, uma sociedade global de risco, na qual se vive cada vez mais uma realidade virtual, tornando-se determinante, portanto, "ponderar a uma nova luz o recurso a meios limitadores dos direitos fundamentais, na

defesa relativamente a perigos gerados pela criminalidade organizada ou pelos atentados contra os fundamentos do Estado" (Mesquita, 2009, p. 152).

A globalização, a Internet e a liberdade de se escrever e consultar o que se bem entende sem constrangimento e sem censura, conduz a um futuro sombrio para a sociedade de risco que assiste à ameaça de "destruição das bases naturais da vida e da incapacidade de reter os perigos da civilização" (Pinheiro, 2015, p. 123), traduzindo-se isso num rápida passagem do risco para a perda: perda de identidade civilizacional, perda de segurança, perda de liberdade democrática. O risco passa a ser omnipresente, sem lugar ou espaço definidos; os danos originados pela natureza dos riscos passam a ser irreparáveis, oriundos das mais diversas fontes: terrorismo, grupos criminosos altamente organizados, entre outras causas sociais; e o risco, pelo carácter incerto que assume e de difícil localização, passa a ser hipotético, sem qualquer base de conhecimento científico-normativo (Pinheiro, 2015).

Nesta sociedade global de risco, onde a Internet ocupa um espaço perigosamente omnipresente, a cibercriminalidade ganha terreno e torna-se uma "ameaça dos tempos modernos" (Proposta de Lei n.º 289/X/4ª). É, pois, necessário dotar a investigação criminal de ferramentas tecnológicas eficientes que possibilitem a intercepção e recolha de informação armazenada em computadores assim como a "preservação expedita e [a] revelação dados de tráfego", dotando as entidades competentes de instrumentos eficazes, adaptados às novas realidades criminógenas, combatendo-as através da sua investigação e julgamento (Proposta de Lei n.º 289/X/4ª).

Muito embora a Lei do Cibercrime tenha materializado medidas de combate ao crime informático ou ao crime relacionado com a informática consideramos que existem outros meios de obtenção de prova que se mantêm de fora do âmbito do que é legalmente permitido e que poderiam ser uma mais valia à investigação de determinados crimes que pela sua gravidade se justificaria a utilização de tais meios de obtenção de prova. Isto porque, no ordenamento jurídico interno, com a Lei do Cibercrime, assistimos a "um impressionismo materialista bem distinto de vias seguidas na Europa e nos Estados Unidos da América a respeito da prova documental e em particular dos registos de comunicações passadas, que compreende ponderações complexas com vista a uma abordagem tecnologicamente neutra dos problemas da privacidade" (Mesquita, 2010, p. 92).

Em bom rigor, dada a evolução do espaço virtual e dos meios tecnológicos, o caminho seguido pela legislação nacional seria o da criação de uma legislação mais intervencionista e mais assertiva no que diz respeito à abertura da excepcionalidade das medidas previstas

para os cibercrimes, mesmo que tal significasse uma ingerência em direitos constitucionalmente consagrados, nomeadamente a privacidade dos dados informáticos do visado pela medida, mas também numa capacidade mais discricionária dos órgãos de polícia criminal no que à investigação criminal diz respeito.

À medida que a tecnologia evolui e o ciberespaço se torna cada vez mais o lugar de eleição para todo o tipo de transações, sejam elas legais ou ilícitas, e à medida que o indivíduo se torna cada vez mais dependente da Internet, é imprescindível criar mecanismos de defesa cada vez mais fortes no sentido de providenciar formas legais de combater os atos cometidos ilicitamente com recurso ao espaço virtual, os quais se revelam cada vez mais astutos. A característica mais proeminente que advém do uso da Internet é que uma vez ali colocada qualquer informação a mesma dissemina-se sem qualquer intervenção humana, revelando todo o seu potencial, para o bem e para o mal.

A problemática com que as polícias se deparam é, como já referimos, com a fungibilidade e volatilidade que envolve a informação ali depositada e com as ferramentas tecnológicas de que dispõem para fazer face a essa característica fugaz da informação virtual. A retenção e apreensão de informação digital é, por isso, determinante para a recolha de elementos probatórios electrónicos que possam incriminar indivíduos da prática de cibercrimes. Mas esta parece ser ainda uma realidade que passa um pouco ao lado do legislador português que optou por uma lei reguladora do cibercrime cuja proteção do núcleo duro de direitos constitucionalmente consagrados continua a ser muito limitativa do trabalho investigatório das polícias e, de uma forma geral, ineficaz no combate aos ilícitos que ocorrem na *Dark Web*. E passamos a explicar porque é que consideramos que a Lei do Cibercrime ficou um pouco aquém do que era expectável de uma lei que viria com o objetivo de mitigar condutas ilícitas virtuais e porque é que, na nossa opinião, se trata de uma lei que pouco ou nada consegue fazer no que diz respeito à realidade da *Dark Web*.

No que à preservação expedita de dados diz concerne, consignada no art. 12.º, à revelação expedita de dados de tráfego, plasmada no art. 13.º, à injunção para apresentação ou concessão do acesso a dados, constante no art. 14.º, à pesquisa de dados informáticos, conforme o art. 15.º, à apreensão de dados informáticos, ínsita no art. 16.º, todos da Lei do Cibercrime, somos da opinião que serão medidas cuja utilidade será nula em matéria de investigação na *Dark Web*. Isto porque as ferramentas usadas para detectar utilizadores estranhos à navegação na *Dark Web*, facilmente bloqueiam o acesso a esse espaço virtual e alertam os utilizadores e possíveis suspeitos, os quais "limpam" qualquer rasto que os possam identificar e incriminar. Os próprios dados armazenados nos sistemas informáticos

estão encriptados, e os responsáveis pelos sites indexados à *Dark Web* muito dificilmente cedem dados dos seus usuários.

Consideramos que o legislador português foi demasiado humilde na elaboração da Lei do Cibercrime, primeiro porque não incluiu os cibercrimes em um capítulo no Código de Processo Penal, segundo porque a Lei do Cibercrime parece pouco audaz no que concerne à intervenção em ambientes digitais mais complexos e cujas águas são mais profundas, como a *Dark Web*. O legislador limita-se a inferir nos sistemas onde os dados poderão estar armazenados não prevendo outras realidades mais voláteis e de difícil alcance. E é precisamente esse ponto que passamos a focar o nosso estudo.

Temos vindo a abordar a cibercriminalidade e agora mais concretamente a *Dark Web* pela sua característica peculiar de conceder anonimato aos seus utilizadores e pela complexidade de se conseguir detectar a "origem do conteúdo ou teor criminoso" (Ramalho, 2013, p. 384), o que transmite à investigação criminal uma certa ineficácia dos seus meios tecnológicos e até dos meios processuais penais atuais (Ramalho, 2013, p. 384). Abrimos aqui um parêntesis para apresentar uma curta definição do que é a *Dark Web*. Segundo Ramalho, a Dark Web trata-se de uma área da Internet que até há relativamente pouco tempo era desconhecida e é "um lado da *Web* dedicado à cibercriminalidade, no qual a detecção dos utilizadores se revela potencialmente inviável e cujo acesso é, em geral, limitado àqueles que instalam um *software* específico, como o *Freenet*, o *The Onion Router* ou o I2P" (Ramalho, 2013, p. 385).

Como já referimos anteriormente, o uso da Internet pode ser direcionado para o bem e para o mal, e a *Dark Web* privilegia os seus utilizadores, por um lado, com a segurança do anonimato que, por motivos político-sociais não podem usar a sua liberdade de expressão (por pertencerem a um estado ditatorial, por exemplo), e por outro lado, com a garantia de impunidade e encobrimento na prática de factos ilícitos (Ramalho, 2013).

No sentido de manter esse anonimato e a liberdade de navegação sem tabus e sem normativos que imponham regras e censurem práticas ilegais e mesmo imorais, existe da parte dos responsáveis pela sua manutenção e desenvolvimento a preocupação em renovar os sistemas software a cada vez que as autoridades policiais se aproximam ameaçadoramente da descoberta de identidades de potenciais utilizadores, procedendo ao lançamento, num curto prazo, de "novas atualizações ou conselhos de utilização que [frustrem] a sua futura exploração pelas forças policiais" (Ramalho, 2013, p. 411). E uma forma encontrada para criar obstáculos às investidas investigatórias criminais online foi a criação de técnicas antiforenses. As técnicas antiforenses traduzem-se na aplicação de

medidas que visam comprometer a disponibilidade ou a utilidade da prova no processo forense, destruindo-a (Ramalho, 2013) inviabilizando e comprometendo a continuidade da investigação criminal.

Nesse sentido foi criado software com a finalidade de eliminar o rasto digital dos utilizadores e perpetradores de ilícitos criminais na *Dark Web*. Entre os mais conhecidos, destaca-se o TOR – *The Onion Router* – que se caracteriza por ser um software mais rápido e que possibilita a navegação num ambiente mais abrangente da Internet, além de que o seu uso permite ocultar o endereço IP do computador e a sua atividade. Este software é assim denominado pelo facto de se ter de ir passando etapas encriptadas – como a casca da cebola – até chegar ao destino final, como forma de mitigar possíveis ameaças ao sistema e à própria navegação na *Dark Web*.

Com a disponibilização do TOR começaram a surgir diversos serviços altamente criminosos: mercados e transações de armas e de drogas, fóruns dedicados ao terrorismo, pornografia infantil, pornografia violenta e mesmo fóruns relacionados com canibalismo (Ramalho, 2013, p. 393). Para facilitar todo este mercado virtual, foi criada uma moeda indetectável do ponto de vista das entidades bancárias, que seria uma forma das polícias conseguirem interceptar suspeitos do cometimento de cibercrimes através de pagamentos e transações online efectuados – a bitcoin. A criação desta moeda possibilitou que o anonimato se mantivesse uma vez que não é necessária a intervenção de entidade bancária, pois a transação decorre anonimamente entre as duas partes envolvidas, sem necessitar de divulgar qualquer informação acerca das suas identificações.

A missão das polícias não se almeja, portanto, facilitada. Em bom rigor, estas técnicas antiforenses levaram a que as polícias de países como os Estados Unidos da América (EUA) e a Alemanha desenvolvessem medidas de monitorização e vigilância secretas de sistemas tecnológicos, sendo que "o acesso secreto a informação contida em sistemas tecnológicos, usando infiltração tecnológica, é um assunto intensamente debatido na arena política e em diversos círculos legais sob o título buscas online/vigilância online" (Acórdão BverfG, 1 BvR 370,595/07, 2008, https://www.bundesverfassungsgericht.de).

Mas a verdade é que estas medidas foram utilizadas isoladamente em alguns casos pela polícia federal [alemã] sem um qualquer poder estatutário específico, e nada se soube sobre a natureza prática da execução prévia dessas buscas online ou até do seu sucesso (Acórdão BverfG, 1 BvR 370,595/07, 2008, https://www.bundesverfassungsgericht.de).

Foi largamente discutida a possibilidade de se fazer a concessão ao Gabinete da Polícia Criminal Federal da utilização das buscas online e sob que pressupostos, no

decorrer das suas atribuições e tarefas e com a finalidade de evitar ameaças de terrorismo internacional, esforços e atividades cujo alvo seria atingir o entendimento internacional ou as relações de paz entre nações, assim como a proteção da segurança interna e da liberdade democrática (Acórdão BverfG, 1 BvR 370,595/07, 2008, https://www.bundesverfassungsgericht.de). O que acabou por acontecer, pois foi introduzido no ordenamento jurídico alemão a autorização para fazer uso de *malware* para efeitos de prevenção de casos de terrorismo.

A dificuldade em obter informação e dados armazenados em sistemas informáticos encriptados relativos a pessoas relacionadas com grupos de terrorismo ou grupos extremistas, tornam o trabalho investigatório criminal tradicional pouco eficaz. O recurso a métodos clássicos de busca de informação e armazenamento de dados em sistemas tecnológicos assim como uma rede baseada numa vigilância de telecomunicações, pode fazer do acesso à informação pretendida uma tarefa quase impossível. Os visados pelas medidas investigatórias tomam sempre precauções contra eventuais tentativas de intrusão nos seus sistemas informáticos e frequentemente atualizam os seus sistemas operativos, sendo facilmente detectada qualquer uma das tentativas de monitorização e vigilância das telecomunicações atrás referida. Para se obter sucesso na infiltração e conseguir a informação pretendida é necessário que essa ingerência seja de certa forma consistente, ou seja, que se prolongue durante algum tempo por forma a que o usuário do sistema operativo visado armazene os dados no seu computador sem os encriptar, e nesse caso a busca online permitirá a recolha dos dados por encriptar, por terem sido acedidos e recolhidos pelas autoridades no momento em que o usuário também acedia aos mesmos.

Esta é uma realidade para a qual o Tribunal Federal Constitucional Alemão começou a estar atento, na medida em que já percepcionou que perante a existência do cibercrime adveio a necessidade de adequar ao caso em concreto medidas investigatórias mais eficazes. Sedimentando o que acabámos de mencionar, "[a]tento à constante surpresa do "admirável mundo novo" das realizações das novas tecnologias (particularmente nos domínios das novas tecnologias e da genética), o Tribunal Constitucional [Alemão] vem naturalmente abrindo o processo penal às possibilidades de investigação sem precedentes que as novas tecnologias oferecem. Fá-lo, porém, sob reserva de um conjunto articulado e exigente de pressupostos e condicionalismos" (Andrade, 2009, p. 22).

Os EUA vão mais longe neste desiderato de proteger a segurança interna do país e a liberdade democrática. Desde o atentado do 11 de setembro que houve um grande desenvolvimento no campo da monitorização, vigilância electrónica e outros meios de

obtenção da prova tecnológica. Num aberto combate ao cibercrime desenvolveram no Laboratório de Inteligência Artificial, no Arizona, um projeto denominado de *Dark Web Project* com o objectivo principal de "recolher e analisar todo o conteúdo gerado por grupos dedicados ao terrorismo internacional, incluindo *websites*, fóruns, salas de *chat*, blogues, redes sociais, vídeos, entre outros, na *Dark Web*" (Ramalho, 2013, p. 411).

O Federal Bureau of Investigation (FBI) também desenvolveu um campo investigatório especializado e direcionado para o combate à cibercriminalidade – *Cyber Division* –, responsável pela investigação de cibercrimes cometidos em território norte-americano e internacional, assim como o terrorismo, e a cibercriminalidade que ponha em risco a segurança interna (de acordo com o site oficial do FBI; https://www.fbi.gov).

Ademais, o FBI utiliza determinadas técnicas digitais secretas como o *malware*, "cuja fundamentação jurídica é por vezes encontrada em leituras algo (es)forçadas da Constituição dos Estados Unidos da América" (Ramalho, 2013, p. 212). A jurisprudência norte-americana é rica em casos em que as autoridades recorrem a métodos ocultos de investigação criminal, nomeadamente as buscas online, o uso de *malware*, entre outras ferramentas tecnológicas, para obter informação que de outra forma se perderia ou não se lograria alcançar, e tratando-se de cibercrimes, o recurso a estes métodos tecnológicos secretos por parte das autoridades é cada vez mais frequente.

Resumidamente, o *malware* pode ser definido como "um programa simples ou auto-replicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático" (Filiol, 2005, p. 99). A implantação de um *malware* providencia o acesso a toda a informação armazenada no sistema informático visado, comprometer toda a sua funcionalidade, causar danos tanto no sistema como ao seu usuário, eliminando, corrompendo, alterando, monitorizar toda a vida do visado, uma vez que tem acesso a toda a sua informação e pode fazer uso dela remotamente, fazendo-se passar pelo próprio. Ademais, a infeção com o *malware* possibilita, por um controlador remoto, saber quais as teclas premidas pelo utilizador do sistema informático (através de *keyloggers*[1]), vigiar a sua atividade em tempo real, escutar

[1] O primeiro caso de utilização de *keyloggers* data de 1999, quando o FBI usou este programa no computador de um conhecido mafioso Nicodemo S. Scarfo por ter conhecimento de que este armazenava no seu computador ficheiros cifrados de elevado valor probatório acerca do seu envolvimento em negócios de jogo ilegal (cfr. USA vs Nicodemo S. Scarfo, 180 F. Supp. 2d 572 (D.N.J.2001), disponível em https://law.justia.com).

as conversas que tem através do *Skype* e até ativar o som e imagem (*webcam*) daquele sistema (Ramalho, 2013).

E essa implantação do *malware* pode fazer-se a partir de três formas: "infeção via suporte físico removível, a infeção via *browser* e a infeção via *download* voluntário" (Ramalho, 2013, p. 207). A infeção via suporte físico removível pode ser feita através de um CD ou uma *pen drive*, sendo útil na investigação criminal em casos em que o servidor não está ligado à Internet, e tem a particularidade de incidir somente no sistema visado e não em outros; a infeção via *browser* resulta da consulta de uma *web page*, aparentemente inofensiva, mas que é composta por um código malicioso que foi ali implantado propositadamente e detetando vulnerabilidades de segurança ou configurações deficientes no sistema, injeta-o com o *malware*; a infeção por via do *download* voluntário traduz-se no download de certos ficheiro, da abertura de anexos que venham no correio electrónico, do download de programas executáveis gratuitos, da atualização de *software,* infetados com *malware*.

São diversos os tipos de *malware* utilizados subrepticiamente e de forma indetectável no âmbito da investigação criminal em ambiente digital, consoante a finalidade que se requeira: os *Trojans*, as *logic bombs*, o *spyware*, os *rootkits*, os vírus, os *worms*, as *blended threats* (Ramalho, 2013), o *Bundestrojaner*, e a partir de 2013 o FBI utilizou o *Magneto*. O *Magneto* trata-se de um *malware* que foi implantado "nos servidores do *Freedom Hosting*, um fornecedor de serviços de armazenamento que continha vários *hidden services* [websites indetectáveis e apenas acessíveis através do TOR] dedicados à pornografia infantil" (Ramalho, 2013, p. 206). O *Bundestrojaner* foi um *malware* utilizado, a partir de 2006, pela polícia alemã no decorrer de inúmeras investigações criminais sobre factos relacionados com terrorismo. Trouxe muita controvérsia e rejeição por parte das autoridades judiciárias, tendo sido solicitado que o Tribunal Constitucional Federal se pronunciasse sobre a constitucionalidade deste meio de obtenção de prova, cuja posição foi de que este programa violava certos direitos e princípios fundamentais. Contudo, como já foi aqui abordado anteriormente esta medida excecional veio a integrar o ordenamento jurídico alemão ficando vinculado o seu uso à prevenção de casos de terrorismo. Em bom rigor, a autorização por legislação de programas *malware* é uma questão de tempo. Sendo a cibercriminalidade transversal a todos os países, existe a necessidade de conjugar esforços no sentido de criar normas que sejam elas também transversais ao nível territorial dos países envolvidos, realçando-se a cooperação internacional que deve existir por força da tal conjugação de esforços.

Por exemplo, a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, que foi transposta para o ordenamento jurídico interno português através da aprovação da Lei do Cibercrime é a materialização dessa vontade europeia em estabelecer normativos convergentes e comuns a todos os Estados-membros.

Mais recentemente, a Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, de 13 de janeiro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, espelha e vem fortalecer o combate à cibercriminalidade, concedendo uma abertura dos meios investigatórios criminais em ambiente digital quando no seu considerando 27) afirma que "os responsáveis pela investigação e pela ação penal relativas aos crimes referidos na presente diretiva deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a intercepção de comunicações, a vigilância discreta, inclusive por meios electrónicos, a monitorização de contas bancárias ou outras investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e a natureza e gravidade dos crimes investigados. Se for caso disso, e de acordo com a legislação nacional, tais instrumentos deverão também incluir a possibilidade de as autoridades policiais utilizarem uma identidade falsa na Internet".

Por enquanto, em Portugal, o *malware* é considerado um meio oculto de obtenção de prova sem assento no ordenamento jurídico. Poderíamos eventualmente considerar que o legislador estaria a levantar o pano à entrada dos meios ocultos de obtenção de prova, em específico ao *malware*, quando refere no n.º 2, do art. 19.º da Lei do Cibercrime que "[s]endo necessário o recurso a meios e dispositivos informáticos", no que diz respeito às ações encobertas, talvez por influência da consagração da utilização de meios técnicos mais eficazes em outros ordenamentos jurídicos. Esta expressão, no nosso entender, vaga, da utilização de meios e dispositivos informáticos não indica a possibilidade de uso de *malware*. Acerca da inadmissibilidade deste meio de obtenção de prova, Mendes defende que "um catálogo dos meios de prova típicos inclui os respectivos regimes e não permite que sejam desrespeitadas as suas regras, a fim de serem criados meios de prova aparentados mas atípicos. (...) Portanto, a única liberdade que existe relativamente à escolha dos meios de prova consiste na possibilidade de selecionar do catálogo dos meios de prova típicos aqueles que forem considerados como adequados ao processo em curso" (Mendes, 2013, p. 174). Posição esta com a qual corroboramos.

Terá de ser o legislador a referir expressamente a legalidade do uso deste tipo de meios ocultos de obtenção de prova, introduzindo-o naquele catálogo de meios de prova

típicos, consagrando-o legalmente como deve ser num Estado de direito democrático. Isto porque a grave danosidade social que este meio oculto de obtenção representa, pela sua ingerência na intimidade da vida privada, na correspondência electrónica, o acesso a dados pessoais armazenados informaticamente, o acesso ao som e à imagem, através da monitorização do computador, merece que essa consagração normativo-legal se enforme de uma especial densidade, além de toda a especificidade de que tal medida se deve revestir, bem como os limites a que deve ser sujeita, tendo como farol o princípio da proporcionalidade e da necessidade (Ramalho, 2013).

Conclusão

Lidamos com um fenómeno criminógeno cada vez mais presente por força da tecnologia disposta livremente. Temos bem presente as dificuldades que as polícias, em geral, têm ao lidar com a cibercriminalidade e as constantes mutações dos meios informáticos ao dispor dos criminosos e que facilitam toda a sua atividade ilícita, aliado ao facto de toda a atividade investigatória criminal estar encapsulada por uma legislação que, apesar de abranger os crimes informáticos e crimes cometidos através de meios informáticos, nos parece "escassa" no que diz respeito ao combate da cibercriminalidade mais profunda: a *Dark Web*. Não menos importante, e que convém aqui ressalvar, é o facto de termos uma legislação cuja vertente garantística dos direitos, liberdades e garantias, dificulta e limita o acesso a informação probatória digital.

Não obstante as últimas alterações normativas ao ordenamento jurídico interno no sentido de incluir a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, somos levados a crer que o legislador ficou um pouco aquém do que seria expectável, deixando um certo sabor amargo pois o que se esperaria, dadas as conjunturas sociais e legais que se têm verificado em outros países e que levam a crer que continuam a trabalhar para se adaptarem à realidade da cibercriminalidade e a introduzirem nos seus ordenamentos jurídicos a consagração de meios técnicos mais eficazes, como o *malware*, para fazer face à evolução do cibercrime. E seria de esperar do legislador português a introdução de profundas alterações normativas idênticas que trouxessem uma lufada de ar fresco à investigação criminal e à possibilidade de aceder a meios tecnológicos mais assertivos e eficientes no ambiente digital. Ademais, cremos que esta será uma realidade que terá de mudar se não quisermos que a cibercriminalidade, aliada a toda a tecnologia avançada de que se mune, ganhe terreno relativamente, não só às polícias, como também ao próprio estado e à liberdade democrática. Quanto às hipóteses teóricas por nós levantadas, e após a exposição que fizemos, cremos que podemos corroborá-las na sua totalidade.

Quando iniciámos o presente estudo tínhamos a noção de que seria difícil conseguir corroborar as hipóteses por nós indicadas, por estar em jogo direitos constitucionalmente protegidos. A essência desses direitos e princípios fundamentais pode ser beliscada pela introdução de meios de prova que, pela sua ingerência, representam um grau de elevada danosidade em áreas mais reservadas da vida privada, da correspondência electrónica, de

dados armazenados num sistema informático, mesmo que acedido remotamente. Contudo, à medida que fomos explorando o tema da cibercriminalidade e toda a problemática que envolve a obtenção de prova digital, fomos tomando consciência de que é necessário proceder a algumas alterações a nível de legislação nacional para que esse combate se torne mais eficaz, como já vem acontecendo com outros países e sobre os quais trouxemos aqui a debate. A evolução tecnológica da cibercriminalidade é uma realidade com a qual as polícias lidam diariamente, e o uso de meios de obtenção de prova mais eficazes – como o *malware* – revelam-se de grande utilidade, como pudemos observar pela exposição que fizemos. Mas para que isso aconteça tem de ser dado o primeiro grande passo: admitir o recurso a meios ocultos de obtenção de prova no ordenamento jurídico interno, revestindo-o de densidade normativa e de requisitos de proporcionalidade, necessidade e excepcionalidade, e sob o escrutínio do juiz que deverá proferir despacho de fundamentação a cada caso.

Referências

Acórdão BverfG, 1 BvR 370,595/07, (2008), disponível em https://www.bundesverfassungsgericht.de.

Acórdão USA vs Nicodemo S. Scarfo, 180 F. Supp. 2d 572 (D.N.J.2001), disponível em https://law.justia.com.

Andrade, M.C. (2009). "*Bruscamente No Verão Passado", a reforma do Código de Processo Penal – observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora.

Código de Processo Penal (Decreto-Lei n.º 78/87, de 17 de fevereiro). Últimas alterações introduzidas pela Lei n.º 33/2019, de 22/05.

Constituição da República Portuguesa (Decreto de 10 de Abril de 1976). Últimas alterações introduzidas pela Lei n.º 1/2005, de 12/08.

Directiva 2011/92/UE do Parlamento Europeu e do Conselho, de 13 de janeiro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, disponível em https://eur-lex.europa.eu

Filiol, E. (2005). *Computer viruses: from theory to applications*. França: Springer.

Gossel, K.H. (1992). As proibições de prova no direito processual penal da República Federal da Alemanha. In *Revista Portuguesa de Ciência Criminal*. Coimbra: Aequitas Editorial Notícias.

Lei n.º 5/2002, de 11 de janeiro (que aprova as medidas de combate à criminalidade organizada e económico-financeira e procede à 2.ª alteração da Lei n.º 36/94, de 29 de setembro, alterada pela Lei n.º 90/99, de 10 de julho, e 4.ª alteração do Decreto-Lei n.º 325/95, de 2 de dezembro, alterado pela Lei n.º 65/98, de 2 de setembro, pelo Decreto-Lei n.º 275-A/2000, de 9 de novembro, e pela Lei n.º 104/2001, de 25 de agosto).

Lei n.º 49/2008, de 27 de Agosto (que aprova a Lei da Organização e Investigação Criminal).

Lei n.º 53/2008, de 29 de agosto (que aprova a Lei de Segurança Interna).

Lei n.º 96/2017, de 23 de agosto (que aprova a Lei de Política Criminal – Biénio de 2017-2019).

Lei n.º 109/2009, de 15 de setembro (que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa).

Mendes, P.S. (2013). *Lições de Direito Processual Penal*, Coimbra: Almedina.

Mesquita, P. D. (2010). *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Wolters Kluwer Portugal-Coimbra Editora.

Pinheiro, A. S. (2015). *Privacy e Protecção de dados pessoais: A construção dogmática do direito à identidade informacional*, Lisboa: Associação Académica da Faculdade de Direito de Lisboa Editora.

Proposta de Lei N.º 289/X/4.ª, disponível em http://app.parlamento.pt.

Ramalho, D. S. (2013). A Investigação Criminal na Dark Web. In *Revista de Concorrência e Regulação*. Coimbra: Almedina.

Ramalho, D.S. (2013). O uso de *malware* como meio de obtenção de prova em processo penal. In *Revista de Concorrência e Regulação*. Coimbra: Almedina.

Susano, H. (2009). *Escutas Telefónicas – Exigências e controvérsias do actual regime*, Coimbra: Coimbra Editora.

Maria de Fátima Magalhães da Rocha
Comissário M/146846