CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW

by CIJIC

EDIÇÃO N.º X – SETEMBRO DE 2020

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

ISSN 2183-729

NOTAS DO EDITOR:

Os últimos tempos, assim e porque não os vindouros, sobressaltam-nos com três complexidades *esdrúxulas*: acesso universal e aberto à Rede e democratização desta; capacitação humana numa era de diluvio informacional; a relação da tecnologia, do digital, ao serviço das organizações e/ou Estado com a pessoa humana.

É inegável que o acesso à Rede é um direito fundamental da pessoa humana. Da mesma forma que a liberdade, a inclusão e democratização do espaço físico possibilitou uma dinamização de valor acrescentado ao elevador social, é já hoje mais do que óbvio, que a inclusão digital trará idênticos efeitos. Quantas mais pessoas acederem à Rede, melhor. E tudo gira em torno de uma característica universal da pessoa humana: o ser social que somos. É, pois, essencial determinarmos, enquanto ente coletivo, a necessidade da prossecução, por via da pólis, de um acesso universal e aberto à Rede. É tema de agenda política.

Preocupam-nos, com efeito, as questões supranacionais que envolvem, desde logo o 5G. O tabuleiro político mundial, neste momento, está partido ao meio. E tal como Harari referiu – ainda que a propósito do combate à pandemia -, é imperioso que saibamos "*criar princípios éticos globais e restaurar a cooperação internacional* (…).". Obviamente, tudo se resume às escolhas que fizermos, *Ie, "(…) Depende das escolhas que fazemos no presente. Os países podem optar por competir por recursos escassos e prosseguir uma política egoísta e*

isolacionista, ou podem escolher ajudarem-se mutuamente através de um espírito de solidariedade global."[1].

Assim, nem *a great firewall* chinesa, uma agenda económica protecionista e isolacionista, ou a pressão e separatismo estaduais servem a humanidade. Não será sobre esta toada *belicista* que a humanidade produzirá ganhos conjuntos. Se é que os almeja produzir. O espírito de solidariedade internacional tem-se perdido na espuma dos dias.

Curiosamente, na era de dilúvio informacional, parece-nos comprometida a capacitação humana. Severa, a incompreensão de que a pessoa humana não pode ser um objeto. Sendo-o, emerge do *trade-off* entre o acesso a um serviço "*free*" e a quantidade de dados pessoais que liberta, não só para lhe aceder como depois no usufruir desse serviço.

Zuboff[2] alerta-nos para o *direct and personal targeting*, um assombro de *direct emotional manipulation* , em que sobressai o modelo de negócio das *big tech trendy* de sempre: o parcelamento informacional da pessoa, vendido a outras corporações como ponto de dados; métricas, perfis, com o intuito de retornar (ao titular dos dados) sob a forma de bem ou comodidade (que julga querer adquirir). Qual rato de laboratório. Uma pirâmide financeira suportada à conta da pessoa titular dos dados pessoais, por esta e para esta.

O resultado concreto, analítico, sob a forma de capitalização bolsista, demonstra-nos que a era da informação, na verdade, não está a funcionar para as massas. Pelo contrário. Erige-se num paradoxo: empobrece as suas (nossas) vidas, quer pelos dados pessoais que *capta* quer pelos bens/comodidades que impinge, e enriquece o pecúlio dos (*famosos*) 1%. A robustez financeira acumulada por tais 1%, por sua vez, demonstra uma capacidade, por si só, de manipulação de pilares fundamentais dos estados de direito democrático: a capacidade para atingir diretamente o núcleo legislativo internacional. Com acesso a leis-fato (à medida), só o Direito poderá colocar travão a esta distopia.

Infelizmente, a erosão, de direitos fundamentais humanos, não fica sustida apenas no aspeto mercantil em que opera a redução da pessoa humana a uma objetificação pronunciada. Intrometida e diligentemente, o próprio Estado passou a focar a pessoa como um "*asset*", como um meio, rasgando os pilares fundacionais de toda a doutrina kantiana.

---

1 Harari @ https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity (ultimo acesso setembro 2020).
2 *The age of surveillance capitalism: the fight for a human future at the new Frontier of power*.

A observação da realidade presente, ainda comprometida pela atualidade da pandemia, não olvida que, à semelhança do *surveillance capitalism*, aqui converge a dualidade relacional humano/tecnologia (digital). Se o Estado se comporta como um ente egoísta, usando as pessoas como mero valor, ponto de dados, métrica ou perfil, miríade informacional para prosseguir determinadas agendas (quais?), o que o distinguirá das organizações privadas que procuram o lucro por todos e quaisquer meios?

Note-se, por exemplo, no caso de Portugal – sendo que é uma prática participada por uma maioria de países democráticos deveras preocupante –, o "estado de vigilância" começa, geralmente, como demonstrando ter um propósito justificado por um "*objetivo*" publicamente aceitável. Daqui deriva para uma moção rotineira, *ie*, uma vez implementado – mesmo que *"a título experimental*" –, passa a fazer parte da rotina diária de todos os cidadãos, planeado e executado de acordo com um cronograma racional, não aleatório, seguindo diretrizes perfeitamente concretas, focado em detalhes, como agregação e armazenamento de *dados*[3].

A justificação, para esta aceitação passiva e obediente, por parte do cidadão, reduz-se a uma vacuidade: "*eu não tenho nada a esconder*…". Contudo, o *estado de vigilância* (à semelhança do homónimo capitalismo) serve quem? O quê? Para quê?

Aquiesçamos, um *estado de vigilância* é um que contempla a vigilância como a solução para a esmagadora maioria das questões sociais complexas. Um *estado de vigilância* é respaldo da incompetência, manifestação de uma viciação por tecnologias (criadas por quem?) e dados (para quê? para quem?), com as limitações aí inerentes.

Tal como na problemática do *surveillance capitalism*, o *estado de vigilância* aparece-nos pressuposto no equilíbrio entre as suas necessidades (quais, porque não são coletivamente sufragadas) e desejos/ansias individuais egoístas. Neste jogo de soma zero para o cidadão - ainda que negociado como uma troca de soma não nula -, a propósito de segurança (ou saúde) prometidos pelo estado, este cede, no todo ou em partes, a sua individualidade. Uma vez tal cedência concretizada, a superioridade informacional granjeada, detida pelo *estado de vigilância,* tende a exaurir os mecanismos democráticos de supervisão do próprio estado, na

3 Podemos trazer à colação, para melhor percebermos, desde logo, os sistemas de videovigilância municipal já implementados. De igual forma, podemos pensar sobre a *vigilância*, embora míope quando o cidadão contribuinte tem uma riqueza pessoal assinalável – e tal miopia poderá explicar a constância de acesso de tais cidadãos a regime excecionais de regularização tributaria - exercida pela Autoridade tributária. Recentemente, uma *novidade*, a *app* stayawaycovid.
Entre reconhecimento facial, pelas cameras de videovigilância; rastreamento através do cartão Mb – incentivado o seu uso massivo também a propósito da pandemia, sendo o *contactless* qual "sabão azul" nas medidas de mitigação da propagação da doença – não só através da localização como também do perfil de consumo, entre outros; à coleta de dados de saúde que a *app* permite, bem como o rastreio geolocalizado; de tudo temos experimentado. Os propósitos são "*claros*": segurança, combate ao crime e saúde. Aliciantes…

medida em que o monopólio do conhecimento lhe permite controlar tudo o que pode ser divulgado. Bem coordenado com uma assinalável retórica de medo, tal *estado* passa a dispor da faculdade de usar os seus poderes para propósitos indiferentes à origem e finalidades registadas aos *baby-step* da sua implementação. Distopia? Sim. E já representada nas nossas vidas.

Urge, pois, contrariar as pulsões totalitaristas de *estados de vigilância*, promotores de exclusão e discriminação, sob pena de o nosso futuro, enquanto ente coletivo, ser irreparavelmente composto por cidadãos desprovidos da sua individualidade intrínseca.

Tal distopia estadual não serve à pessoa humana. A luta convoca-nos a todos.

O núcleo não pode, em momento algum, ser desfocado da sua essência: Estado ao serviço da pessoa. Tecnologia ao serviço da pessoa. É pela pessoa que o Estado se materializa. É para a pessoa que o Estado se organiza numa comunhão de direito democrático. É por um Estado que promove e prossegue o cardápio de direitos, liberdades e garantias fundamentais da pessoa que cumpre lutar. De igual forma, o recurso à ferramenta de auxílio – a tecnologia (digital) – pode e deve ser feito sempre que a finalidade seja construir um ente coletivo em que a pessoa é e sempre, também pela sua individualidade intrínseca, um fim em si mesmo. É por tal *futuro por design*, na disponibilidade da pessoa e pela pessoa humana que devemos concentrar o nosso esforço coletivo.

Nesta nova edição da Cyberlaw by CIJIC, perseguidos por tais inquietações, tivemos o ensejo de provocar os autores participantes à procura de juízos sobre a realidade desafiante que convoca a sociedade atual. E futura. Entre a inteligência artificial e a *algocracia* e os desafios que estas convocam ao Direito (e aos juristas); passando pelo crime de violência domestica num contexto de abuso (mais uma forma de abuso) através das redes sociais e a proteção jurídico-penal que a vida privada exigem; à utilização de *benware* como meio de neutralização das técnicas e medidas antiforenses que os criminosos usam; à engenharia do "direito penal sobre rodas" e ao agente inteligente automóvel num contexto de um certo desarranjo terminológico - todos escritos em língua portuguesa - e ante as responsabilidades – que já demos conta oportunamente – impondo-se-nos a difusão de conteúdo em inglês escrito, juntamos três temas desafiantes: *State surveillance; fake news & social networks; open banking*.

Como era expectável, *ab initio*, os temas são desafiantes. Para todos. São, como sempre, abertos a colaboração múltipla e, de preferência, participada. A prova foi, quer-nos parecer, superada com mestria.

Entretanto abre-se a janela da próxima edição, para Março de 2021. Não sem antes sublinhar que, nos próximos tempos, ante os critérios definidos pelo corpo diretivo e pelo editor, em parceria com a Associação académica da faculdade de direito de lisboa, passaremos a dispor de um número da revista, anualmente, em formato de papel.

Resta-me, por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2020

Nuno Teixeira Castro

CYBERLAW
by CIJIC

DA ADMISSIBILIDADE DA UTILIZAÇÃO DE BENWARE NO DIREITO PORTUGUÊS

ON THE ADMISSIBILITY OF THE USE OF BENWARE UNDER PORTUGUESE LAW

DUARTE RODRIGUES NUNES *

* Juiz de Direito, Professor Convidado da Universidade Europeia (Direito penal), Doutor em Direito pela Faculdade de Direito de Lisboa, Investigador do Centro de Investigação de Direito Penal e Ciências Criminais e do Centro de Investigação Jurídica do Ciberespaço.

RESUMO

A utilização das medidas antiforenses e de meios de comunicação como as comunicações por VoIP pelos criminosos dificulta de sobremaneira a investigação criminal. Por isso, as autoridades têm de utilizar meios que neutralizem essas dificuldades. Um desses meios é a instalação sub-reptícia de programas informáticos que permitam infiltrar sistemas informáticos para obter informações relevantes para a investigação (*benware*). A lei portuguesa não prevê expressamente a utilização de *benware*, apenas existindo uma referência implícita ao uso de *benware* no art. 19.º, n.º 2, da Lei n.º 109/2009. Apesar disso, a utilização de *benware* é admissível à luz do Direito português, embora seja preferível que o legislador preveja expressamente essa possibilidade na lei.

Palavras-chave: Buscas *online* – Cibercrime – investigação criminal – prova digital – Direito à confidencialidade e à integridade dos sistemas técnico-informacionais.

ABSTRACT

The use of anti-forensic measures and means of communication, such as VoIP communications, by criminals, makes criminal investigation extremely difficult. Therefore, the authorities must use means that can counteract these difficulties. One of these means is the surreptitious installation of computer programs that permit to infiltrate computer systems in order to obtain information that is relevant to the investigation (benware). Portuguese law does not expressly provide for the use of benware. There is only an implicit reference to the use of benware in art. 19, no. 2, of Law no. 109/2009. Nevertheless, the use of benware is admissible under Portuguese Law, although it is preferable that the legislator expressly provides for this possibility in the Law.

Keywords: Remote computer searches – Cybercrime – Criminal investigation – Digital evidence – Right in Confidentiality and Integrity of Information Technology Systems.

Sumário: 1. Introdução e colocação do problema; 2. A utilização de *benware* no Direito comparado; 3. A utilização de *benware* no Direito português; 4. Conclusões. Bibliografia. Jurisprudência.

1. INTRODUÇÃO E COLOCAÇÃO DO PROBLEMA

Devido à crescente utilização das chamadas medidas antiforenses (encriptação das mensagens, esteganografia, utilização de *firewalls*, *botnets*, VPN ou *proxies*, da *Dark Web*, de programas como o TOR, *Freenet* e I2P e de criptomoedas, etc.] e de meios de comunicação como as comunicações por VoIP[1] por parte dos agentes de crimes informáticos (precisamente com a finalidade de se protegerem das medidas de prevenção criminal e de investigação criminal levadas a cabo pelas autoridades), torna-se cada vez mais necessária a utilização, pelas autoridades, de mecanismos e dispositivos que permitam neutralizar a utilização de medidas antiforenses e a proteção proporcionada pela utilização de meios de comunicação como as comunicações por VoIP.

Um desses mecanismos e dispositivos é precisamente a instalação sub-reptícia de programas informáticos (vírus, *worms*, "cavalos de Troia", *keyloggers*, *backdoors*, *spyware*, etc.) que permitam que as autoridades se infiltrem num sistema informático[2] alheio, com o intuito de obter informações relevantes para a investigação (incluindo a prevenção criminal), que, de outro modo, não poderiam ou dificilmente poderiam obter[3].

1 O VoIP (*Voice over Internet Protocol*) é uma forma de comunicar "telefonicamente" através da Internet mediante a utilização de um *software* específico (*Skype Google Talk, Facebook, Whatsapp, Telegram, Viber, Gizmo, Fring, Adphone, Camfrog, MinoCall, VoipBuster, Voipdiscount UOL VoIP*, etc.), permitindo também a comunicação sonora e imagética. Apesar de a comunicação por VoIP se assemelhar a uma chamada telefónica, o seu funcionamento é radicalmente diverso, pois a comunicação via VoIP processa-se nos seguintes termos: um dos interlocutores liga-se a um determinado provedor de acesso à Internet (através de um qualquer sistema informático), autentica-se no programa de VoIP através de um endereço e um código de acesso e "telefona" ao outro interlocutor. As palavras e imagens trocadas entre ambos são convertidas em sinal digital e esses dados são encriptados pelo sistema de VoIP e passam a ser *peer to peer*, circulando os pacotes de dados encriptados na Internet até chegarem ao destinatário, sendo então desencriptados; a comunicação é instantânea, não consiste em nenhuma "caixa de cartas" (como sucede com o correio eletrónico) nem passa por nenhum computador central, o que significa que tudo passa por uma rede de *peer to peer* em contínua modificação e sem nunca estar sob o controlo de terceiros (incluindo a empresa que fornece o serviço de VoIP).

2 Na aceção do art. 2.º, al. a), da Lei n.º 109/2009, de 15 de setembro: «*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*».

3 Cfr. JONATHAN MAYER, Constitutional Malware, pp. 6-7.

No fundo, trata-se de programas que são, usualmente, subsumidos ao conceito de *malware*[4]. Todavia, optamos por denominar este tipo de programas informáticos, quando usados para fins de prevenção ou repressão criminais pelas autoridades (fins legítimos e absolutamente essenciais em qualquer Estado de Direito), *benware*[5].

Tendo em conta a necessária "clandestinidade" da instalação do *benware* nos sistemas informáticos visados – que faz antever o cariz "oculto" das medidas investigatórias cuja execução essa instalação visa permitir –, a utilização do *benware* está intimamente ligada à questão dos métodos "ocultos" de investigação criminal[6]. A instalação do *benware* terá de ser precedida pela "colocação" (e ulterior instalação) do programa no sistema informático na sequência de o utilizador visitar uma determinada página da Internet (em regra, alojada na *Dark Web*) controlada pelas autoridades (permitindo-lhes instalar o programa de forma sub-reptícia) (*watering hole tactic*)[7], por meio do envio do programa de instalação para o sistema informático visado através de um *e-mail* contendo um anexo infetado ou um *link* para um sítio da Internet aparentemente legítimo (sendo o sistema informático infetado quando o utilizador clica no *link*) (*social engeneering tactic*) ou mediante a procura e o consequente aproveitamento de alguma fragilidade na segurança do sistema informático (*máxime* falhas

4 Designação que resulta da aglutinação de sílabas das palavras inglesas *malicious* e *software* e que significa programa informático malicioso, precisamente porque se trata de programas informáticos que visam permitir a quem os 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, em regra para fins criminosos (preparação ou execução de crimes ou apagamento de provas de crimes cometidos, incluindo o ataque informático a sistemas informáticos pertencentes às autoridades).

5 *Benign software*: *software* benigno.

6 Os métodos "ocultos" de investigação criminal são os métodos de investigação criminal «*que configuram «uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto ou dele se apercebam*» e que, por isso, «*continuam a agir, interagir, expressar-se e comunicar de forma "inocente", fazendo ou dizendo coisas de sentido claramente autoincriminatório ou incriminatório daqueles que com elas interagem ou comunicam*», podendo ser "ocultos "por natureza" ou apenas eventualmente "ocultos", consistindo os primeiros naqueles métodos que, pela sua própria natureza, só podem ser utilizados "às ocultas" (ações encobertas, escutas telefónicas, etc.) e os segundos naqueles que tanto podem ser utilizados de forma "aberta" como "às ocultas" (*v.g.* a fixação e comparação de perfis de ADN) (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 202-203).

7 Esta técnica de introdução do *benware* no sistema informático suscita a questão da "autorização para todos os sistemas informáticos" ("*All computers" warrant*), dado que todas as pessoas que acedam ao *website* (incluindo pesssoas inocentes) verão os seus sistemas informáticos infetados com o *benware* e sujeitos a buscas *online*, o que suscita questões relacionadas com a proporcionalidade da medida, mais concretamente questões relacionadas com a *probable cause* no Direito norte-americano (cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 762 e ss., e JONATHAN MAYER, Constitutional Malware, p. 60) e com a exigência da existência de uma suspeita *objetiva* e fundada nos termos do Direito português enquanto pressuposto geral, embora implícito, de todos os meios de obtenção de prova que restrinjam direitos fundamentais de forma intensa (cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 472 e ss.).

de segurança que algum programa ou aplicação instalados contenha)[8] ou mesmo através de atualizações de *software* que o visado permita que sejam efetuadas no sistema informático (reconduzível à *social engeneering tactic*)[9]. No entanto, parece-nos que os criminosos cautelosos dificilmente abrirão o *link* do *e-mail* que contém o *benware*, pelo que o programa terá de ser instalado por alguma das outras formas que referimos.

Tanto a instalação do *benware* como a execução da operação proporcionada pela instalação do *benware* terão de evitar a "atuação" de dispositivos de segurança instalados no sistema informático (antivírus, antispyware, *firewalls*, etc.), a fim de que não apaguem o *benware* nem o detetem ("avisando" o utilizador)[10].

A utilização de *benware* é essencial no caso da busca *online* (*online-Durchsuchung*), que consiste na infiltração sub-reptícia e à distância num sistema informático para observação/monitorização da sua utilização e leitura e eventual cópia dos dados nele armazenados ou acessíveis a partir dele, podendo consistir num único acesso (*Daten-Spiegelung*) ou ocorrer de forma contínua e prolongada no tempo (*Daten-Monitoring*)[11]. A busca *online* caracteriza-se (e diferencia-se das buscas "clássicas" previstas nos arts. 174.º, 176.º e 177.º do CPP e da pesquisa de dados informáticos prevista no art. 15.º da Lei n.º 109/2009, de 15 de setembro) por ser realizada *online*, à distância, "às ocultas", com recurso a meios técnicos e implicar a prévia instalação sub-reptícia, no sistema informático visado, de um programa informático do tipo "cavalo de Troia" (que constitui um mero ato preparatório da execução da busca *online*)[12]. No entanto, ainda que constitua um ato

8 Cfr. MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 410, DAVID SILVA RAMALHO, "O uso de *malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, pp. 205 e ss., JONATHAN MAYER, Constitutional Malware, pp. 13 e ss., e DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 736-737, 739 e 741-742.

9 Cfr. JONATHAN MAYER, Constitutional Malware, p. 15, refere que a colocação do *benware* (para posterior instalação e pesquisa) poderá ocorrer de qualquer forma, dando como exemplos "adicionais" a entrada sub-reptícia no local onde está o sistema informático e instalação "presencial" do *software* e a apreensão do sistema informático de um criminoso participante na atividade criminosa sob investigação e executar a diligência a partir desse sistema.

10 Cfr. JONATHAN MAYER, Constitutional Malware, pp. 15-16.

11 Cfr. COSTA ANDRADE, "Bruscamente no Verão Passado" p. 166, e também em "Art. 194.º", *in* Comentário Conimbricense, I, 2.ª Edição, p. 1103, PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 541, BÄR, TK-Überwachung, p. 75, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 803 (com mais indicações bibliográficas), e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 226-227, e SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, 1, p. 61.

12 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 541, COSTA ANDRADE, "Bruscamente no Verão Passado", p 166, e BÄR, TK-Überwachung, p. 75. Relativamente ao modo de instalar esse *sotftware*, *vide* BÄR, *Op. Cit.*, pp. 75-76.

preparatório da execução da busca *online* e/ou de outros meios de obtenção de prova (como a intervenção nas comunicações eletrónicas mediante a vigilância nas fontes e a vigilância acústica e/ou ótica), a instalação de *benware* restringe o direito à confidencialidade e à integridade dos sistemas técnico-informacionais[13], sendo essa a raiz do problema da admissibilidade da utilização de *benware* na ausência de norma legal que a preveja expressamente.

Do mesmo modo, a utilização de *benware* é igualmente essencial no caso da vigilância nas fontes (*Quellen-Telekommunikationsüberwachung* ou *Quellen-TKü*), que consiste na interceção de comunicações (que terão de estar em curso[14]) que sejam encriptadas antes da sua saída do sistema informático "emissor" e desencriptadas depois da sua receção no sistema informático "recetor" (como sucede, por exemplo, nas comunicações por VoIP), sendo assim designada precisamente pelo facto de a interceção só pode ocorrer antes da encriptação ou depois da desencriptação dos dados (pois, após a sua encriptação e antes da sua desencriptação, será impossível de realizar), o que requer a instalação de *software* adequado no sistema informático visado (*v.g.* programas do tipo "cavalo de Troia"). Também na vigilância nas fontes é necessária a prévia instalação de *benware*, o que constitui um mero ato preparatório da execução da interceção das comunicações[15].

Uma outra situação – esta eventual (pois depende do modo como a vigilância acústica e/ou ótica, sob a forma de registo de voz e imagem[16] ou de interceção de comunicações entre presentes[17], é levada a cabo) –, em que poderá ser necessária a utilização de *benware* é precisamente a vigilância acústica e/ou ótica quando deva/tenha de ser levada a cabo mediante

13 Cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 292, e MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 409-410.

Acerca do direito à confidencialidade e à integridade dos sistemas técnico-informacionais e da sua aplicabilidade no Direito português, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 240 e ss.

14 Cfr. MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 409, e também em "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 420.

15 Como refere BÄR, TK-Überwachung, p. 55, a instalação do *software* necessário para intercetar as comunicações "na fonte" é um ato preparatório da realização das "escutas", sendo em tudo similar à colocação de um localizador de GPS no veículo do visado ou dos microfones no interior da residência onde irá ser realizada a intervenção nas conversações entre presentes; daí que tenhamos de considerar que a instalação sub-reptícia do *software* é um ato que está incluído, por natureza, na autorização da realização das escutas [contra, HOFFMANN-RIEM, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme e BUERMEYER/BÄCKER, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO, p. 434).

16 Nos termos do art. 6.º da Lei n.º 5/2002, de 11 de janeiro.

17 Nos termos do art. 189.º, n.º 1, do CPP.

a ativação (sub-reptícia) da câmara e/ou do microfone do sistema informático (computador, *smartphone*, *tablet*, etc.) (*captatore informatico*).

Apesar do disposto no art. 19.º, n.º 2, da Lei n.º 109/2009, não nos parece que a utilização de *benware* seja necessária nas ações encobertas *ex se*, sem prejuízo de poder ocorrer – e ocorrer – relativamente a (outros) meios de obtenção de prova utilizados no âmbito de ações encobertas.

Ao contrário do que sucedeu noutras ordens jurídicas, o legislador português não regula expressamente a utilização de *benware*, o mesmo sucedendo com as buscas *online*, a vigilância nas fontes e a ativação sub-reptícia da câmara e/ou do microfone do sistema no âmbito do registo de voz e imagem ou da interceção de comunicações entre presentes.

Deste modo, o problema central deste estudo prende-se com a admissibilidade da utilização do *benware* na investigação criminal à luz do Direito português.

2. A UTILIZAÇÃO DE BENWARE NO DIREITO COMPARADO

Começando pelo Direito alemão[18], o §100a I e III[19] da *Strafprozessordnung* (StPO) prevê expressamente a vigilância nas fontes, que segue o mesmo regime jurídico das escutas telefónicas, devendo ser autorizada pelo Juiz ou, em situações de urgência, pelo Ministério Público (com ulterior ratificação do Juiz no prazo de 3 dias úteis)[20] sempre que existam suspeitas fundadas da prática de um crime previsto no §100a II e a diligência seja indispensável para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou a prova seja, de outra forma, impossível ou muito difícil de obter[21]. Pode ser dirigida contra o arguido ou suspeito ou contra pessoas em relação às quais existam suspeitas fundadas de que recebem ou transmitem mensagens destinadas ou provenientes do arguido ou suspeito[22] durante um período até 3 meses, renovável por períodos até 3 meses[23], mediante despacho fundamentado nos termos do §100e IV StPO, jamais podendo ser obtidas informações subsumíveis à esfera íntima tal como delimitada pela teoria das três esferas[24]. A lei não prevê o modo de instalação do *benware*[25]. Anteriormente à Reforma da StPO de 2017, o §100a StPO não continha qualquer referência à vigilância nas fontes[26].

---

18 O Direito alemão não prevê expressamente a ativação sub-reptícia da câmara e/ou do microfone do sistema informático no âmbito da vigilância acústica (*Lauschangriff*) nem no âmbito da vigilância ótica (*Spähangriff*), o que leva MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 421, a considerar que o uso do *captatore informatico* – que restringe o direito à confidencialidade e à integridade dos sistemas técnico-informacionais – não é admissível à luz do Direito germânico.

19 Na redação que lhe foi dada pela Reforma da StPO de 2017.

De acordo com o §51 II da *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* (*Bundeskriminalamtgesetz* – BKAG), *in* http://www.gesetze-im-internet.de/bkag_2018/ (consultada em 09/07/2020), o *Bundeskriminalamt* (Polícia Judiciária Federal) pode realizar vigilâncias nas fontes mediante autorização judicial na prevenção do terrorismo.

20 §100e I StPO.

21 §100a I 1 StPO.

22 §100a III StPO.

23 §100e I StPO.

24 §100d StPO.

25 Como nota MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 410.

26 Por isso e porque a instalação de *benware* restringe o direito à confidencialidade e à integridade dos sistemas técnico-informacionais [cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 292, MARCUS KÖHLER, "100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 409-410, e Sentença do *Bundesverfassungsgericht* de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07)] –, a admissibilidade da vigilância nas fontes era controvertida na Doutrina alemã. Com efeito, alguns autores pronunciavam-se pela inadmissibilidade, argumentando que, sendo a vigilância nas fontes similar à busca *online* ao nível da execução (o que excluiria a aplicação do §100a StPO), como a StPO não previa este meio de obtenção de prova, também não seria admissível recorrer à vigilância nas fontes em sede de investigação criminal (cfr. KLESCZEWSKI, "Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von Strafprozessualen Ermittlungseingriffen im Internet", *in* Zeitschrift für die gesamte Strafrechtswissenschaft, 2012, p. 742, SINGELNSTEIN, "Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche

Por sua vez, o §100b da StPO[27] prevê a busca *online* em matéria de repressão penal, a qual deve ser autorizada por 3 juízes da Secção (*Kammer*) criminal do *Landgericht* (Tribunal

Datenverarbeitung&Co", *in* Neue Zeitschrift für Strafrecht, 2012, p. 599, HOFFMANN-RIEM, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme, e BUERMEYER/BÄCKER, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO, pp. 439-440).

Diversamente, um outro setor da Doutrina pronunciava-se no sentido da admissibilidade, argumentando que havia que diferenciar ambas as realidades, pois a vigilância nas fontes configura uma intervenção nas comunicações eletrónicas que, por razões *meramente técnicas*, poderá ter de ocorrer antes da encriptação ou após a desencriptação dos dados (mas nunca durante o processo comunicacional) e, ao passo que a busca *online* inclui o rastreio do sistema informático na sua globalidade, a vigilância nas fontes limita-se à interceção de comunicações realizadas através de VoIP, sendo que a prévia instalação dos programas necessários para a interceção das comunicações no sistema informático funcionava como uma *Annexkompetenz* relativamente ao §100a, nos termos da qual a autorização para a realização das intervenções nas comunicações legitimava a prévia instalação dos programas informáticos (cfr. BÄR, TK-Überwachung, p. 75, e NACK, "§100a", *in* Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 6.ª Edição, p. 476).

27 Anteriormente à entrada em vigor da atual versão do §100b da StPO (no âmbito da Reforma da StPO de 2017), a busca online apenas estava prevista em sede de prevenção criminal do terrorismo (cfr. §§20k VII – atual §49 – da BKAG).

Todavia, ao nível da repressão criminal, apesar de a lei não prever/regular a busca *online*, não existia unanimidade na Jurisprudência alemã, encontrando-se arestos que se pronunciavam pela admissibilidade, aplicando o regime das buscas com base numa interpretação atualista e considerando que a busca *online* não constituía uma restrição intensa de direitos fundamentais [*v.g.* Sentença do *Bundesgerichtshof* de 21/02/2006 (3 BGs 31/06, 3 BJs 32/05 - 4 - (12) - 3 BGs 31/06)] e arestos que consideraram que este meio de obtenção de prova não era admissível, por ausência de previsão legal [*v.g.* Sentença do *Bundesgerichtshof* de 31/01/2007 (StB 18/06).

Por seu turno, o *Bundesverfassungsgericht*, na sua marcante Sentença de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07), analisou a constitucionalidade do §5 II 11, da Lei de Proteção da Constituição do Estado da Renânia do Norte-Vestefália (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*) na versão introduzida pela Lei de 20/12/2006 à luz do art. 2 I, conjugado com os arts. 1 I, 10 I e 19.º I 2, da Lei Fundamental Alemã (Grundgesetz – GG).

O §5 II 11, da Lei de Proteção da Constituição do Estado da Renânia do Norte-Vestefália permitia ao *Bundesamt für Verfassunfsschutz* (Gabinete Federal para a Proteção da Constituição) aceder, de forma sub-reptícia e remota, a sistemas informáticos de indivíduos suspeitos de cometerem ilícitos criminais, a fim de pesquisar os dados aí armazenados ou acessíveis através desse sistema, monitorizar a sua utilização de forma prolongada no tempo e até controlar o próprio sistema informático mediante a prévia instalação sub-reptícia de programas que permitissem esse acesso (*benware*). Nos termos do §3 da Lei de Proteção da Constituição (*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz* – BVerfSchG), *in* http://www.gesetze-im-internet.de/bverfschg/index.html (consultada em 09/07/2020), compete ao *Bundesamt für Verfassunfsschutz* recolher e analisar informações relativas a atividades ilícitas que atentem contra o Estado de Direito (a "*livre ordem democrática fundamental*"), a existência ou a segurança do Estado federal ou Federação (*Bund*) ou de um Estado federado (*Land*) ou que visem prejudicar ilegalmente a administração dos órgãos constitucionais do Estado federal ou de um Estado federado ou respetivos membros, bem como a atividades que atentem contra a segurança interna ou os interesses externos da República Federal da Alemanha ou de serviços secretos estrangeiros.

O *Bundesverfassungsgericht* considerou que, no caso das buscas *online*, os direitos fundamentais ao sigilo das telecomunicações, à inviolabilidade do domicílio e à autodeterminação informacional não proporcionavam uma tutela eficaz, pelo que, à semelhança do que sucedera com o direito à autodeterminação informacional [Sentença de 15/12/1983 (1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83,1 BvR 440/83 e BvR 484/83)], criou um novo direito fundamental (que, no entendimento do Tribunal, é restringido, e de forma intensa, pela busca *online*): o direito fundamental à confidencialidade e à integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

E o *Bundesverfassungsgericht* considerou também que a referida norma não cumpria as exigências constitucionais de clareza e certeza jurídica e de proporcionalidade. E estabeleceu as coordenadas que, pela intensidade da restrição do direito à confidencialidade e à integridade dos sistemas técnico-informacionais que o recurso às buscas *online* acarreta, uma futura regulamentação das buscas *online* deveria observar.

Deste modo, de acordo com o Tribunal, só será legítimo o recurso às buscas *online* mediante autorização judicial e desde que exista uma suspeita fundada da existência de um perigo concreto para um bem jurídico particularmente relevante (o Tribunal refere a vida, a integridade física e a liberdade, bem como os bens jurídicos

estadual de 2.ª instância) da área da sede do departamento do Ministério Público competente para a investigação ou, em situações de urgência, pelo Presidente dessa Secção Criminal (com ulterior ratificação de 3 juízes da Secção Criminal no prazo de 3 dias úteis)[28] sempre que existam suspeitas fundadas da prática de um crime previsto no §100b II (cujo catálogo é muito mais restritivo do que o catálogo do §100a) e a diligência seja indispensável para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou a prova seja, de outra forma, impossível ou muito difícil de obter[29]. Pode ser dirigida contra o arguido ou suspeito ou contra pessoas em relação às quais existam suspeitas fundadas de que o arguido ou suspeito utiliza os seus sistemas informáticos e desde que a intervenção apenas nos sistemas informáticos do arguido se mostre insuficiente para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou para a obtenção da prova[30], durante um período até 1 mês, renovável por períodos até 1 mês (e, caso a duração total se prolongue por mais de 6 meses, as ulteriores renovações terão de ser autorizadas pelo *Oberlandesgericht*, o Tribunal supremo de cada um dos *Länder*[31] alemães)[32], mediante despacho fundamentado nos termos do §100e IV StPO, jamais podendo ser obtidas informações subsumíveis à esfera íntima tal como delimitada pela teoria das três esferas[33].

Quanto ao Direito italiano[34], prevê-se, no art. 266, 2 e 2-bis, do *Codice di procedura penale*, o uso do *captatore informatico*[35], que consiste num *software* do tipo "cavalo de Troia"

---

da comunidade cuja lesão ou ameaça de lesão possa pôr em causa os fundamentos ou a existência do Estado ou da Humanidade), devendo a lei conter salvaguardas para proteção da área nuclear da privacidade (a esfera íntima). E, na sua Sentença de 20/04/2016 (1 BvR 966, 1140/09), o *Bundesverfassungsgericht* reafirmou este entendimento, ao afirmar que as restrições intensas de direitos fundamentais por via da utilização de métodos "ocultos" de investigação criminal (como é o caso das buscas *online*) na prevenção criminal só são admissíveis se observarem as exigências do princípio da proporcionalidade, devendo ser limitadas à proteção de bens jurídicos importantes e apenas quanto existir uma suspeita fundada da verificação de um perigo concreto para um desses bens jurídicos, efetivo controlo das operações e suficientes salvaguardas para a proteção da intimidade e do sigilo profissional (com o dever de eliminação dos dados obtidos), só podendo ser restringida a esfera jurídica de terceiros em situações muito limitadas.

Ainda previamente à previsão do recurso à busca *online* na StPO, o *Bundesverfassungsgericht* afirmou a constitucionalidade da interpretação ampla do conceito de telecomunicações do §100a StPO no sentido de incluir a monitorização da navegação na Internet [cfr. Sentença de 06/07/2016 (2 BvR 1454/13)].

28 §100e II StPO.

29 §100b I 1 StPO.

30 §100b III StPO. Todavia, se forem atingidos outros sistemas informáticos, mas essa circunstância for tecnicamente inevitável, as provas obtidas são válidas (cfr. ROXIN/SCHÜNEMANN, Strafverfahtensrecht, 27.ª Edição, p. 292, e MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 422).

31 Estados federados.

32 §100e II StPO.

33 §100d StPO.

34 No Direito italiano não existe qualquer previsão expressa da busca *online* nem da vigilância nas fontes.

35 Anteriormente à previsão legal do *captatore informatico*, as *Sezioni Unite* da *Suprema Corte de Cassazione* haviam fixado jurisprudência no sentido da admissibilidade da utilização deste meio tecnológico nas investigações relativas à criminalidade organizada, entendendo que se trata apenas de um meio de execução das interceções de comunicações entre presentes, dispensando o art. 13 do *Decreto legge* n.º 151 de 1991, convertido pela *Legge* n.º

que é sub-repticiamente instalado num sistema informático para permitir a ativação do microfone para audição/gravação de conversações, a geolocalização do sistema informático e a ativação da câmara para vigilância ótica (incluindo tirar fotografias). O *captatore informatico* constitui um meio de execução da interceção de comunicações entre presentes e não um meio de obtenção de prova "autónomo", sendo utilizado nos casos em que é admissível a interceção de comunicações entre presentes, que tanto pode ocorrer em locais que gozam da tutela constitucional do domicílio (locais indicados no art. 614 do *Codice penale*) como em locais privados que não gozam dessa tutela.

Nos termos do art. 266, 2 e 2-bis, do *Codice di procedura penale*, a interceção de comunicações entre presentes (e o *captatore informatico*) terá de ser autorizada pelo Juiz ou, em caso de urgência, pelo Ministério Público (com ulterior ratificação do Juiz no prazo de 48 horas contadas da comunicação, que deve ocorrer no prazo máximo de 24 horas) por despacho fundamentado[36] sempre que existam suspeitas fundadas da prática de um crime previsto no art. 266, 1 e 2-bis, e a diligência seja indispensável para a descoberta da verdade ou do paradeiro do arguido ou suspeito ou a prova seja, de outra forma, impossível ou muito difícil de obter[37]. No caso da interceção de comunicações entre presentes "domiciliária", terão de existir fundados indícios de que a atividade criminosa (também) está a ocorrer nesse local[38]; todavia, nos termos do art. 13 do *Decreto legge* n.º 151 de 1991, convertido pela *Legge* n.º 203 de 1991, quando se trate de processos relativos à criminalidade organizada, é possível a realização de interceções de comunicações entre presentes "domiciliárias" mesmo que a atividade criminosa não esteja a ocorrer nesse local.

Nos casos de *periculum in mora* em que a autorização seja dada pelo Ministério Público e seja utilizado o *captatore informatico*, terá de estar em causa a investigação de crimes previstos no art. 51, 3-bis e 3-quater (*grosso modo*, crimes no âmbito da criminalidade organizada e do terrorismo), e crimes contra a Administração Pública praticados por

---

203 de 1991, a exigência de que a atividade criminosa não esteja a ocorrer no local protegido pela tutela do domicílio onde deverá ser realizada a interceção (derrogando, assim, o art. 266, 2, do *Codice di procedura penale*), pelo que nada impede a sua utilização (tendo em conta a natureza "itinerante" dos sistemas informáticos da atualidade como o *smartphone*, o *tablet* ou o computador); diversamente, nos demais casos, em que há que observar o disposto no art. 266,2, a *Corte de Cassazione* considerou que já não será admissível, uma vez que, no momento da concessão da autorização, não é possível prever em que locais "domiciliários" o *captatore informatico* poderia vir a ser instalado no sistema (cfr. Sentença das *Sezioni Unite* da *Suprema Corte de Cassazione* de 28/04/2016-01/07/2016, n.º 26889).

No mesmo sentido, cumpre ainda referir as Sentenças da *Suprema Corte di Cassazione* de 30/05/2017-20/10/2017, n.º 48370 (Sez. V), 08/03/2018-09/10/2018, n.º 45486 (Sez. VI), e 25/06/2019-17/12/2019, n.º 50972 (Sez. I).

36 Art. 267, 1, 2 e 2-bis, do *Codice di procedura penale*.

37 Art. 267, 1, do *Codice di procedura penale*.

38 Art. 267, 2, do *Codice di procedura penale*.

funcionários públicos ou por pessoas encarregadas do serviço público puníveis com pena de prisão cujo limite máximo seja igual ou superior a 5 anos[39] (o que significa que o legislador considera que a utilização do *captatore informatico* aumenta a danosidade da interceção de comunicações entre presentes, ao ponto de restringir o âmbito dos casos em que o Ministério Público pode lançar mão de um procedimento *ex abrupto* face às situações de interceção de comunicações entre presentes em que não é utilizado o *captatore informatico*).

No que tange à duração da medida, nos termos do art. 267, 3, do *Codice di procedura penale*, após o Juiz autorizar (ou ratificar a autorização do Ministério Público) a interceção de comunicações entre presentes (com ou sem utilização do *captatore informatico*), o Ministério Público terá de proferir um despacho em que determina a modalidade da interceção e a sua duração[40]. A interceção de comunicações entre presentes não pode ter lugar uma duração superior a 15 dias, embora podendo ser renovada[41].

Relativamente ao Direito espanhol, as buscas *online* (*registros remotos sobre equipos informáticos*) estão previstas nos arts. 588 *septies* a, b e c da *Ley de Enjuiciamiento Criminal* (LECr). Nos termos do art. 588 *septies* a, n.º 1, da LECr, a utilização de dados e códigos de identificação e a instalação de *software* que permita o acesso remoto mediante o uso de meios técnicos a um sistema informático ou suporte externo de armazenamento em massa de dados informáticos sem conhecimento do seu proprietário ou utilizador[42] terão de ser autorizadas pelo Juiz[43] e desde que se trate da investigação de crimes cometidos no âmbito de organizações criminosas, de terrorismo, de crime cometidos contra menores ou incapazes, contra a Constituição, de traição e relativos à defesa nacional ou de crimes cometidos com utilização de meios informáticos ou de qualquer outra tecnologia da informação ou das comunicações ou serviço de comunicações[44]. O âmbito da busca *online* poderá ser ampliado

39 Art. 267, 2-bis, do *Codice di procedura penale*.
40 Cfr. TONINI, Manuale di Procedura Penale, 12.ª Edição, p. 385.
41 Art. 267, 3, do *Codice di procedura penale*.
42 De acordo com LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, p. 14, a busca *online* prevista nos arts. 588 *septies* a, b e c da LECr não permite a interceção de comunicações informáticas.
43 Devendo o despacho de autorização observar as exigências do n.º 2 desse art. 588 *septies* a e dos arts. 588 *bis* c, n.º 3, e 588 *sexies* c, n.º 1, igualmente da LECr. LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, pp. 19-20, refere que o legislador espanhol, ao contrário do que sucede no art. 588 *ter* d (relativo à intervenção nas comunicações telefónicas e telemáticas), não previu a possibilidade de lançar mão de procedimentos *ex abrupto* em situações de *periculum in mora* nem se mostra possível aplicar o mencionado preceito às buscas *online*.
44 De acordo com LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, pp. 9, 10 e 11, terá de existir uma suspeita fundada (e não apenas uma suspeita inicial e muito menos conjeturas ou suposições) da prática de um desses crimes (que, para existir, poderá implicar a realização prévia de outras diligências), sendo que a lei não fixa qualquer exigência quanto à moldura penal aplicável ao crime em causa (cfr. pp. 14-15).

mediante autorização judicial sempre que existam razões fundadas para crer que os dados que as autoridades pretendem obter estão armazenados noutro sistema informático o noutra parte do sistema informático alvo da busca *online*[45]. A busca *online* só pode ser autorizada por um prazo máximo de 1 mês, prorrogável até ao limite máximo de 3 meses[46].

No Direito norte-americano não existe legislação específica relativamente à utilização de *benware* na investigação criminal, à exceção da *Rule 41* das *Federal Rules of Criminal Procedure*, cuja epígrafe é *Search and Seizure* (buscas e apreensões), e na qual foi introduzida, em 2016, uma regulamentação específica para as pesquisas em dispositivos informáticos e apreensões de dados informáticos armazenados em tais dispositivos realizadas de forma remota.

Contudo, já antes dessa alteração legislativa se admitia a utilização das buscas *online*, contanto que tal não violasse a Quarta Emenda à Constituição.

Inicialmente, a Jurisprudência do *Supreme Court of the United States* entendia que só existiria violação da Quarta Emenda nos casos em que a busca e/ou a apreensão implicassem a entrada física em propriedade alheia (*Physical Trespass Doctrine*)[47]. Todavia, o mesmo Tribunal, na marcante Sentença Katz *v.* United States[48], abandonou a *Physical Trespass Doctrine* e ampliou o âmbito de proteção da Quarta Emenda, entendendo que essa tutela, para além de não se limitar à apreensão de bens corpóreos e incluir também a interceção e gravação de conversações e comunicações[49], não abrangia apenas espaços, mas também as pessoas, contanto que exista, no caso concreto, uma expectativa razoável de privacidade da pessoa visada (pelo que a violação da Quarta Emenda não depende da entrada física das autoridades na propriedade privada, mas da existência de uma expectativa razoável de privacidade); e, na situação *sub juditio* nessa Sentença, o *Supreme Court of the United States* considerou que a realização de escutas através de um dispositivo eletrónico de escuta e gravação colocado na

45 Art. 588 *septies* a, n.º 3, da LECr.

46 Art. 588 *septies* c da LECr. LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, p. 18, critica a redação da lei, entendendo que deveria ter clarificado a questão do início da contagem do prazo da duração da busca *online*, que, pela sua natureza, implica a prévia instalação do *benware*, podendo decorrer um determinado lapso de tempo até que as autoridades logrem essa instalação tornando o prazo máximo de 3 meses insuficiente; por isso, a autora entende que a contagem do prazo deveria iniciar-se a partir da instalação do *benware*.

47 Cfr. Sentenças Olmstead *v.* United States (1928) e Goldman *v.* United States (1942) do *Supreme Court of the United States*.

48 Sentença Katz *v.* United States do *Supreme Court of the United States* (1967).

49 Como o *Supreme Court of the United States* também já havia afirmado na sua Sentença Silverman *v.* United States (1961).

parte externa da cabine telefónica a partir da qual o arguido realizara chamadas telefónicas relativas a apostas ilegais estava abrangida pelo âmbito de tutela da Quarta Emenda.

Ainda de acordo com a referida Sentença Katz *v.* United States, a existência de uma expectativa razoável de privacidade depende da verificação de dois pressupostos cumulativos: (1) a pessoa que invoca a Quarta Emenda ter uma expectativa subjetiva de privacidade e (2) a Sociedade reconhecer que essa expectativa é razoável[50].

Para além da demonstração da existência de uma expectativa razoável de privacidade, quem invocar a Quarta Emenda terá de demonstrar que a sua privacidade e/ou a sua propriedade (e não a de terceiros) foram lesadas pela busca e/ou pela apreensão, o que implica saber se essa pessoa alegou que um seu interesse legalmente protegido foi efetivamente lesado (*injury of fact*) e se essa alegação assenta nos seus direitos ou interesses ou num direito ou interesse de um terceiro[51].

Assim, considera-se que as buscas e apreensões (incluindo as pesquisas em sistemas informáticos e as apreensões de dados informáticos[52]) restringem a Quarta Emenda[53], que proíbe a realização de buscas e apreensões desrazoáveis (devendo a razoabilidade da diligência ser aferida à luz da decisão que concede a autorização e do modo como a diligência é executada)[54], embora apenas sendo aplicável às buscas e apreensões realizadas no território

50 Cfr. Sentença Katz *v.* United States do *Supreme Court of the United States* (1967).
51 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 39-40, e Sentença Rakas *v.* Illinois do *Supreme Court of the United States* (1978).
52 Cfr. THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, p. 208, SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 12-13, e Sentenças United States *v.* Lin Lyn Trading, Ltd. do *United States Court of Appeals, 10th Circuit* (1998) e United States *v.* Hunter do *United States Court for the District of Vermont* (1998).
53 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 40 e ss., THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 197-198, ERIC D. MCARTHUR, "The Search and Seizure of Privileged Attorney-Client Communications", *in* University of Chicago Law Review, Vol. 72, p. 732, e Sentenças Andresen *v.* Maryland do *Supreme Court of the United States* (1976), Rakas *v.* Illinois do *Supreme Court of the United States* (1978), Klitzman, Klitzman and Gallagher v. Krut do *United States Court of Appeals, 3rd Circuit* (1984), United States *v.* Lin Lyn Trading, Ltd. do *United States Court of Appeals, 10th Circuit* (1998), Ferguson *v.* City of Charleston do *United States Court of Appeals, 4th Circuit* (2001), United States *v.* Hunter do *United States Court for the District of Vermont* (1998) e United States v. Skeddle do *United States District Court for the North District of Ohio, Western Division* (1997).
54 Cfr. LAFAVE/ISRAEL/KING/KERR, Criminal Procedure, 5.ª Edição, p. 151, SHELLY MOTT DIAZ, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, p. 60, e Sentenças Andresen *v.* Maryland do *Supreme Court of the United States* (1976), Zurcher *v.* Stanford Daily do *Supreme Court of the United States* (1978) e United States *v.* Hunter do *United States Court for the District of Vermont* (1998)

dos Estados Unidos ou que incidam sobre sistemas informáticos ou dados informáticos localizados no território do Estados Unidos[55].

Entende-se que se estará perante buscas e apreensões desrazoáveis, por exemplo, nos casos em que o seu objeto seja excessivamente amplo[56] (*máxime* no caso de mandados de busca "gerais") ou quando sejam realizadas sem autorização judicial (*warrant*) ou fora do âmbito das exceções à exigência de autorização judicial (*v.g.* consentimento do visado, situação de *periculum in mora* para a obtenção da prova ou para a segurança dos agentes ou de terceiros ou o local a buscar não se situar no território dos Estados Unidos)[57].

Contudo, a Quarta Emenda apenas protege contra buscas e apreensões que sejam realizadas pelas autoridades ou por particulares atuando sob a direção das autoridades[58], não incluindo os casos em que as buscas e as apreensões são realizadas por particulares sem qualquer direção das autoridades nem as buscas e apreensões realizadas pelas autoridades quando se limitem a "replicar" buscas e/ou apreensões anteriormente realizadas por particulares que não atuem sob a direção das autoridades[59]. Todavia, a tutela da Quarta Emenda já abrange a parte da busca ou apreensão em que as autoridades vão além da mera "replicação" da busca ou apreensão realizada pelo particular *motu proprio*[60].

---

55 A Jurisprudência norte-americana tem entendido que a Quarta Emenda não abrange as buscas e apreensões e, deste modo, as buscas *online* e outros acessos remotos a sistemas informáticos e/ou dados informáticos localizados no Estrangeiro e pertencentes a estrangeiros não residentes nos Estados Unidos, como aconteceu nos Casos Gorshkov e Ivanov, em que se considerou não abrangida pela tutela da Quarta Emenda, uma busca *online* realizada pelo FBI nos sistemas informáticos (localizados na Rússia) de dois cidadãos russos (Gorshkov e Ivanov) não residentes nos Estados Unidos sem autorização judicial (e sem que existisse qualquer situação que a dispensasse) (acerca deste caso, *vide* SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, pp. 49-50).

56 Cfr. SHELLY MOTT DIAZ, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, pp. 68-69, e Sentenças Andresen *v.* Maryland do *Supreme Court of the United States* (1976), Klitzman, Klitzman and Gallagher v. Krut do *United States Court of Appeals, 3rd Circuit* (1984), United States *v.* Hall do *United States Court of Appeals, 7th Circuit* (1998), United States *v.* Hunter do *United States Court for the District of Vermont* (1998) e O' Connor *v*. Johnson do *Supreme Court of Minnesota* (1979).

57 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 7 e 16-17.

58 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 46-47, THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 232 e ss., e Sentenças Smith *v.* Maryland do *Supreme Court of the United States* (1979), United States *v.* Jacobsen do *Supreme Court of the United States* (1984) e United States *v.* Hall do *United States Court of Appeals, 7th Circuit* (1998).

59 *V.g.* quando um técnico informático a quem o visado entregou o computador para reparação visiona os ficheiros armazenados nesse computador e informa as autoridades acerca daquilo que encontrou e as autoridades apreendem o computador e pesquisam os dados aí armazenados.

60 Cfr. THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 241 e ss., e Sentenças Walter *v.* United States do *Supreme Court of the United States* (1980), United States *v.* Jacobsen do *Supreme Court of the United States* (1984) e United States *v.* Hall do *United States Court of Appeals, 7th Circuit* (1998).

A Quarta Emenda não impede, em absoluto, a realização de buscas e apreensões visando pessoas que não sejam arguidas nem suspeitas, desde que exista autorização judicial[61] (*warrant*) ou uma exceção à exigência de autorização judicial (*v.g.* consentimento do visado, situação de *periculum in mora* para a obtenção da prova ou para a segurança dos agentes ou de terceiros ou o local a buscar não se situar no território dos Estados Unidos[62]), *probable cause* (*i.e.*, uma probabilidade fundada de que a diligência permitirá obter provas do crime sob investigação[63], visando-se evitar *phishing expeditions*[64]) e o local a ser alvo da busca e os elementos a apreender estejam suficientemente especificados na autorização judicial, para que as autoridades que executarem a diligência saibam, com razoável certeza, quais os locais a buscar e quais os elementos a apreender[65].

No caso de apreensões de elementos probatórios que estejam na posse de um terceiro, o proprietário que tiver confiado esses elementos a esse terceiro não tem legitimidade para

---

61 De acordo com as Sentenças Chimel v. California (1969) e Coolidge v. New Hampshire (1971) do *Supreme Court of the United States*, a autorização do Juiz, enquanto entidade neutra, visa precisamente obstar ao arbítrio nas restrições da Quarta Emenda.

62 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 16-17, e Sentença Coolidge v. New Hampshire do *Supreme Court of the United States* (1971).

63 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 13, e DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 761.

64 Cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 761, e Sentenças Katz *v.* United States (1967), Chimel v. California (1969) e Coolidge v. New Hampshire (1971) do *Supreme Court of the United States*.

65 Cfr. TERI DOBBINS BAXTER, "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 43 e 64, ERIC D. MCARTHUR, "The Search and Seizure of Privileged Attorney-Client Communications", *in* University of Chicago Law Review, Vol. 72, p. 732, THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, p. 270, SHELLY MOTT DIAZ, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, p. 61, e Sentenças Zurcher *v.* Stanford Daily do *Supreme Court of the United States* (1978), United States *v.* Hunter do *United States Court for the District of Vermont* (1998), National City Trading Corp. *v.* United States do *United States Court of Appeals, 2nd Circuit* (1980) e O' Connor *v.* Johnson do *Supreme Court of Minnesota* (1979).

No entanto, relativamente à delimitação do âmbito das buscas e dos documentos a serem apreendidos, o *Supreme Court of the United States*, na Sentença Andresen *v.* Maryland (1976), entendeu que existem perigos graves inerentes à execução de uma busca e apreensão dos documentos que não estão necessariamente presentes numa busca que vise a apreensão de objetos físicos (cuja relevância é mais facilmente verificável), visto que, no caso das buscas e apreensões de documentos, irão ser analisados documentos irrelevantes para a investigação (para identificar e apreender aqueles cuja apreensão foi autorizada), o que impõe a adoção de procedimentos que permitam minimizar as restrições da privacidade. Mas, o Tribunal também referiu que, no caso de investigações complexas, é possível que o esquema criminoso só possa ser provado reunindo muitos elementos de prova, incluindo elementos que, considerados isoladamente, pouco ou nada demonstrariam, sendo que a complexidade de um esquema criminoso não pode ser usada como um escudo para evitar a deteção quando exista causa provável para crer que um crime foi cometido e que as provas do seu cometimento estão na posse do visado. Daí que, em tais casos, uma busca e apreensão com base num mandado que delimite o âmbito da diligência de uma forma mais "geral" não viole a Quarta Emenda. De acordo com SHELLY MOTT DIAZ, *Op. Cit.*, p. 60, e THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, p. 197, este entendimento tem sido seguido pelos demais Tribunais para sustentarem a admissibilidade de buscas e apreensões de documentos com um objeto mais amplo.

impugnar a medida por violação da Quarta Emenda, salvo se demonstrar a existência de uma expectativa razoável de privacidade[66]. Assim, por exemplo, a pessoa contra quem forem utilizadas as provas obtidas através de uma busca e apreensão visando um espaço pertencente a um terceiro inocente não tem legitimidade para invocar a violação da Quarta Emenda[67], o mesmo sucedendo com quem ocupe ilegitimamente o local que é objeto da busca[68].

No que tange especificamente às buscas *online* (*remote computer searches*), vem-se entendendo que as buscas *online* constituem uma busca (*search*) para efeitos de proteção no âmbito da Quarta Emenda, pelo que os cidadãos e estrangeiros residentes no território dos Estados Unidos têm uma expectativa razoável de privacidade (*reasonable expectation of privacy*) relativamente aos seus sistemas informáticos e dados informáticos[69], salvo se tiverem exposto tais dados ao conhecimento de terceiros através da instalação e utilização de *software* de partilha de dados que exponha pelo menos parte desses dados a outros

66 Cfr. Sentenças Couch *v.* United States (1973), United States *v.* Miller (1976) e Rakas *v.* Illinois (1978), todas do *Supreme Court of the United States.*

67 Cfr. Sentença Rakas *v.* Illinois do *Supreme Court of the United States* (1978).

68 Assim, Sentença Rakas *v.* Illinois do *Supreme Court of the United States* (1978).

69 Cfr. SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, 1, pp. 51-52 e 61, e também em Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 8, 10 e 12, DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 755 e ss., JONATHAN MAYER, Constitutional Malware, pp. 19 e ss., 26 e 39, e Sentenças Riley *v.* California do *Supreme Court of the United States* (2014), Guest *v.* Leis do *United States Court of Appeals, 6th Circuit* (2001), United States *v.* Lifshitz do *United States Court of Appeals, 2nd Circuit* (2004), United States v. Forrester do *United States Court of Appeals, 9th Circuit* (2007), United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008) e Commonwealth *v.* Cormier do *Massachussets Superior Court* (2011).

De notar que DEVIN M. ADAMS, *Idem*, pp. 756 e ss., considera, inclusivamente, que também o ato de envio do *benware* para o sistema informático visado restringe a Quarta Emenda; diversamente, JONATHAN MAYER, *Idem*, p. 52, entende que tal deverá ser aferido caso a caso, excluindo a restrição da Quarta Emenda nos casos de envio remoto do *benware* no sistema informático visado.

Mas já será diferente quanto à instalação do *benware* e à neutralização dos dispositivos de proteção do sistema informático (para não apagarem nem "avisarem" o visado acerca da presença do *benware*), em que se entende que essa neutralização, ao constituir uma quebra da integridade do sistema informático, restringe a Quarta Emenda (cfr. JONATHAN MAYER, *Idem*, p. 53); contudo, se esta é a regra, existem exceções, que dispensam a obtenção de uma autorização judicial para instalar o *benware*, como sucede, por exemplo, com as redes de partilha de ficheiros *peer-to-peer* quando se "anunciem" no âmbito de redes públicas, mas não quando tal ocorra no âmbito de redes privadas, ainda que sem qualquer proteção [cfr. JONATHAN MAYER, *Idem*, pp. 53, 54, e Sentenças United States v. Ganoe do *United States Court of Appeals, 9th Circuit* (2008) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008)]; JONATHAN MAYER, *Idem*, pp. 54 e ss., refere outras possíveis exceções (*in abstracto*), mas que rejeita na sua totalidade.

Por fim, JONATHAN MAYER, *Idem*, pp. 21 e ss., leva a cabo uma análise da proteção, no âmbito da Quarta Emenda, das buscas *online* na vertente da "Quarta Emenda centrada no dispositivo" ("*Device-Centric Fourth Amendment*") – tendo em conta o entendimento tradicional relativo ao âmbito de proteção da Quarta Emenda – e na vertente da "Quarta Emenda centrada nos dados" ("*Data-Centric Fourth Amendment*") – tendo em conta a nova conceção resultante da Sentença Katz *v.* United States –, acabando por concluir que a Quarta Emenda tutela, quer o sistema informático *ex se* quer os dados informáticos.

utilizadores[70] ou do envio de mensagens após a chegada destas ao destinatário[71]. E entende-se também que a mera circunstância de aceder à Internet não retira ao respetivo titular a expectativa razoável de privacidade[72], o mesmo valendo nos casos em que outras pessoas tenham, ocasionalmente, acesso ao sistema informático[73].

Todavia, tem-se entendido que as informações disponibilizadas pelo cliente ao fornecedor de serviços (provedor) não estão protegidas pela Quarta Emenda em virtude de não existir qualquer expectativa razoável de privacidade a partir do momento em que as partilhou com um terceiro (o fornecedor de serviço)[74], o que inclui os dados relativos à subscrição do serviço[75], os dados de tráfego e os endereços de IP dos *websites* que o utilizador da Internet visita[76] e o tamanho dos ficheiros e outros dados que não sejam relativos ao conteúdo a que o fornecedor de serviço tenha forçosamente acesso no âmbito da prestação de serviços[77].

Também as buscas *online* têm de ser alvo de uma autorização judicial ("*Trojan warrant*") – que terá de identificar (caso seja conhecido[78]) o(s) sistema(s) informático(s) que irá(ão) ser alvo da pesquisa e os ficheiros que deverão ser procurados e apreendidos (especificando o tipo de dados que os agentes policiais estão autorizados a buscar e apreender, como, por exemplo, indicando que irão ser buscados dados relativos a pornografia infantil, a terrorismo ou a tráfico de estupefacientes) – e terá de existir *probable cause* (ou seja, terão de existir circunstâncias objetivas que sejam suficientes para criar num *bonus pater familias* a convicção de que irão ser encontradas informações relevantes para a investigação no sistema

70 Cfr. SUSAN BRENNER, "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, 1, p. 61, e Sentença United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).
71 Cfr. Sentenças United States *v.* Lifshitz do *United States Court of Appeals, 2nd Circuit* (2004) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).
72 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 10-11, e Sentença United States *v.* Heckenkamp do *United States Court of Appeals, 9th Circuit* (2007).
73 Cfr. Sentenças Leventhal v. Knapek do *United States Court of Appeals, 2nd Circuit* (2001) e United States *v.* Heckenkamp do *United States Court of Appeals, 9th Circuit* (2007).
74 Cfr. Sentenças Guest *v.* Leis do *United States Court of Appeals, 6th Circuit* (2001) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).
75 Assim, Sentenças Guest *v.* Leis do *United States Court of Appeals, 6th Circuit* (2001) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).
76 Cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 754-755, e Sentenças United States v. Forrester do *United States Court of Appeals, 9th Circuit* (2007) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).
77 Cfr. Sentenças United States v. Forrester do *United States Court of Appeals, 9th Circuit* (2007) e United States *v.* Perrine do *United States Court of Appeals, 10th Circuit* (2008).
78 Em tais situações, JONATHAN MAYER, Constitutional Malware, p. 59, considera que será sempre possível definir um conjunto de critérios objetivos baseados nas circunstâncias do caso sob investigação, a fim de que o *benware*, quando for instalado, o seja num sistema informático que satisfaça as exigências da Quarta Emenda em matéria de *probable cause*, a fim de obstar a *fishing expeditions*.

informático que irá ser pesquisado[79])[80]. Contudo, no caso da autorização judicial, a mesma poderá ser dispensada sempre que ocorra alguma das exceções à exigência da autorização, designadamente o consentimento do visado, a verificação de uma situação de *periculum in mora* (*exigent circumstances)* quanto à segurança dos agentes policiais ou de terceiros ou quanto à perda de provas essenciais para a investigação ou o sistema informático que irá ser alvo da busca *online* não se encontrar no território dos Estados Unidos[81].

Discutida é a aplicação da *Plain View Doctrine*[82], existindo autores e Jurisprudência que negam a sua aplicabilidade às pesquisas em sistemas informáticos (incluindo as buscas *online*), apenas sendo admissível apreender os dados informáticos especificados na autorização da apreensão (*Special Doctrine*)[83], mas também não faltando Doutrina e Jurisprudência que afirmam a sua aplicabilidade em tais situações[84].

Quanto à duração da busca *online*, nos termos da *Rule 41* das *Federal Rules of Criminal Procedure*, a sua duração máxima é de 14 dias, findos os quais, ou é obtida nova autorização judicial ou haverá que desinstalar o *benware*.

A Jurisprudência norte-americana também já admitiu a vigilância ótica mediante a ativação *online* da câmara do sistema informático na Sentença In re Warrant to Search Target

---

79 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 13, e DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 66-67.

80 Assim, SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 14, DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 760 e ss., e Sentenças Katz *v.* United States (1967), Chimel v. California (1969), Coolidge v. New Hampshire (1971) e Riley *v.* California (2014) do *Supreme Court of the United States* e United States v. Wey do *United States District Court for the Southern District of New York* (2017).

81 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, pp. 16-17, e Sentenças Riley *v.* California do *Supreme Court of the United States* (2014), United States *v.* Gorshkov do *United States District Court for the Western District of Washington* (2001) e United States v. Ivanov do *United States District Court for the District of Connecticut* (2001).

82 De acordo com a *Plain View Doctrine*, poderão ser apreendidos elementos que sejam encontrados no decurso de uma busca que não tenham qualquer relação com o crime cuja investigação motivou a diligência, desde que se verifiquem três pressupostos: (1) uma prévia intrusão lícita (*v.g.* uma busca ou pesquisa informática regularmente autorizadas), (2) o objeto em causa ter sido observado no estrito âmbito da diligência definido pela autorização judicial (*v.g.* se for procurada uma arma com determinadas dimensões, não será lícito aos investigadores realizarem buscas em locais em que tal arma, pelas suas dimensões, manifestamente não possa estar, pelo que o objeto fortuitamente encontrado terá de estar num local em que a arma procurada pudesse ser encontrada) e (3) o caráter criminoso do objeto fortuitamente encontrado ser manifesto (acerca da *Plain View Doctrine*, *vide* THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 275-276).

83 Cfr. SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 17 (embora apenas quanto às buscas *online*, pelo facto de serem realizadas com utilização de meios técnicos), e Sentença United States v. Carey do *United States Court of Appeals, 10th Circuit* (1999).

84 Cfr. THOMAS K. CLANCY, "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 275-276, e Sentença State *v.* Schroeder do *Court of Appeals of Wisconsin* (2000).

Computer at Premises Unknown do *United States District Court for the Southern District of Texas*[85]. O Tribunal, aplicando os critérios definidos pelo *Supreme Court of the United States* na Sentença Berger *v.* New York[86] relativamente às escutas telefónicas e à vigilância acústica e constantes do *Wiretap Act* (§2511 do *United States Code*[87]) e aplicados, por analogia, à vigilância ótica pelo *United States Court of Appeals (5th Circuit)* na Sentença United States *v.* Cuevas-Sanchez[88], admitiu a vigilância ótica mediante a ativação *online* da câmara do sistema informático, embora considerando que terá de existir *probable cause* e autorização do Juiz, devendo tal autorização (1) justificar a insuficiência de outros meios de obtenção de prova para obter as provas no caso concreto (seja porque foram utilizados sem êxito seja porque, de acordo com uma apreciação razoável, se afiguram *ab initio* insuficientes ou perigosos), (2) descrever especificamente o tipo de comunicação que se pretende intercetar (*in casu*, o tipo de imagem que se pretende recolher) e o crime concretamente em causa no caso concreto, (3) indicar a duração da autorização, que não deve exceder o necessário para atingir o objetivo da autorização nem, em qualquer caso, mais de 30 dias (embora sejam possíveis extensões) e (4) identificar as medidas que serão adotadas para garantir que a vigilância será limitada apenas à prossecução dos fins para os quais a autorização foi concedida[89].

85 Sentença In re Warrant to Search Target Computer at Premises Unknown do *United States District Court for the Southern District of Texas* (2013) (concordando, *vide* JONATHAN MAYER, Constitutional Malware, pp. 73-74).

86 Sentença Berger *v.* New York do *Supreme Court of the United States* (1967).

87 Relativo ao crime de interceção de comunicações telefónicas, orais e eletrónicas [*in* *https://www.law.cornell.edu/uscode/text/18/2511* (consultado em 20/07/2020)].

88 Sentença United States *v.* Cuevas-Sanchez do *United States Court of Appeals, 5h Circuit* (1987); já anteriormente, o *2nd Circuit* do mesmo *United States Court of Appeals,* na Sentença United States *v.* Biasucci, adotara o mesmo entendimento.

89 No fundo, exige-se aquilo que a Doutrina e a Jurisprudência norte-americanas designam por "*super warrant*" da Quarta Emenda (relativos aos meios de obtenção de prova mais intensamente restritivos dos direitos fundamentais protegidos por esta Emenda) face ao *warrant* que a mencionada Emenda impõe, por exemplo, em matéria de buscas (incluindo as revistas) e apreensões "tradicionais". De referir que JONATHAN MAYER, Constitutional Malware, pp. 75 e ss., entende que a autorização para a realização de uma busca *online*, pela sua grande danosidade em termos de restrição de direitos fundamentais, deverá observar os requisitos do "*super warrant*" e não os requisitos (menos exigentes) do *warrant* "normal".

3. A UTILIZAÇÃO DO *BENWARE* NO DIREITO PORTUGUÊS

O Direito português não contém qualquer referência expressa à utilização de *benware* na investigação criminal, tal como também não prevê a busca *online*, a vigilância nas fontes e a vigilância acústica e/ou ótica mediante a ativação da câmara e/ou do microfone do sistema informático. Apenas encontramos uma referência implícita ao uso de *benware* no art. 19.º, n.º 2, da Lei n.º 109/2009, relativo às ações encobertas em ambiente informático-digital ou *online*, em que se prevê a possibilidade de utilização de meios e dispositivos informáticos (onde podemos incluir os programas subsumíveis ao conceito de *benware*) no âmbito das ações encobertas *online*[90].

Assim, haverá que analisar a admissibilidade da vigilância nas fontes, as busca *online* e da vigilância acústica e ótica (sob a forma de interceção de comunicações entre presentes e/ou de registo de voz e imagem) com utilização de *benware* para ativação da câmara e/ou do microfone do sistema informático visado.

Começando pela vigilância nas fontes, sendo a nossa lei omissa quanto a essa possibilidade, não existe acordo na Doutrina quanto à sua admissibilidade[91]. Pela nossa parte, consideramos que é admissível, embora devamos repartir a nossa análise em duas vertentes. Quanto à primeira vertente (que se refere à interceção de comunicações *ex se*), não se

90 Consideramos que esta norma não pode constituir a norma habilitante para o uso de *benware* e, consequentemente, para a realização de buscas *online*, vigilância nas fontes e/ou vigilância acústica e/ou ótica mediante a ativação da câmara e/ou do microfone do sistema informático.

Em primeiro lugar, pela leitura que fazemos da norma, não foi essa a finalidade com que o legislador terá criado essa norma (contra, DAVID SILVA RAMALHO, "O uso de *malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, p. 236), que, sem prejuízo de a considerarmos supérflua, apenas tem a finalidade de clarificar a possibilidade de, no âmbito das ações encobertas *online*, serem utilizados meios e dispositivos informáticos, tanto para execução da ação encoberta *ex se* (*v.g.* a ação encoberta ser executada com a utilização de *Cybercops* em vez de pessoas reais) como para a utilização de outros meios de obtenção de prova autónomos (desde logo, as buscas *online*). Por isso, a previsão legal terá de constar de outra norma.

E, em segundo lugar, como refere DAVID SILVA RAMALHO, *Op. Cit.*, pp. 231 e ss., o art. 19.º, n.º 2, da Lei n.º 109/2009 padece da clareza, previsibilidade e precisão exigíveis em sede de restrições de direitos fundamentais quanto aos pressupostos e requisitos da utilização de *benware*, bem como da realização de buscas *online*, vigilância nas fontes e vigilância acústica e/ou ótica mediante a ativação da câmara e/ou do microfone do sistema informático (que, para mais, são meios de obtenção de prova/métodos "ocultos" de investigação criminal fortemente restritivos de direitos fundamentais).

91 Considerando que o art. 18.º da Lei n.º 109/2009 permite a vigilância nas fontes, *vide* PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 119, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 572, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 156; contra, entendendo que, inexistindo previsão legal expressa, a vigilância nas fontes não é admissível, COSTA ANDRADE, "Bruscamente no Verão Passado" p. 165, e DAVID SILVA RAMALHO, Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 339 e ss.

levantam particulares dúvidas quanto à admissibilidade, contanto que estejam verificados os pressupostos legais previstos no art. 18.º da Lei n.º 109/2009.

Por seu turno, quanto à segunda vertente (que se refere à instalação do *benware*), que é a que suscita as divergências doutrinais quanto à admissibilidade que referimos, não vemos em que medida a falta de previsão legal da possibilidade de instalação sub-reptícia de *benware* no sistema informático visado para permitir a intervenção nas comunicações (antes da encriptação dos dados no sistema "emissor" ou depois da sua desencriptação no sistema "recetor") constitui fundamento para negar a admissibilidade. Por várias razões.

Em primeiro lugar, a vigilância nas fontes configura uma intervenção nas comunicações eletrónicas que, por razões *meramente técnicas*, requer a prévia instalação de *benware*, sendo que a instalação do *benware* restringe direitos fundamentais de uma forma pouco intensa.

Em segundo lugar, a instalação de *benware* configura um mero ato preparatório da intervenção nas comunicações por VoIP, à semelhança do que sucede com a duplicação da linha do número do telefone visado pela escuta telefónica. Ou seja, a instalação de *benware*, para além de constituir uma restrição de direitos fundamentais muito pouco significativa (sobretudo quando comparada com a restrição que resulta da intervenção nas comunicações), é um ato que está incluído, por natureza, na interceção de comunicações eletrónicas quando realizadas por VoIP.

Em terceiro lugar, o art. 18.º da Lei n.º 109/2009 refere-se a "interceções de comunicações" (em sistemas informáticos) sem operar qualquer distinção, exclusão ou ressalva, pelo que, ao permitir a interceção de quaisquer comunicações realizadas por meio de um sistema informático (onde se incluem as comunicações por meio de VoIP), permite também a interceção de comunicações através de VoIP. E, se o legislador, conhecendo a necessidade de instalar previamente *benware* no sistema informático visado, optou por permitir a interceção de quaisquer comunicações realizadas por meio de um sistema informático (sem operar qualquer distinção, exclusão ou ressalva), não faz qualquer sentido afirmar-se que, como a interceção de comunicações através de VoIP requer a prévia instalação de *benware*, o art. 18.º da Lei n.º 109/2009 não permite a interceção de comunicações nessas circunstâncias.

Em quarto lugar, poderia aduzir-se que a vigilância nas fontes, pelo facto de requerer a prévia instalação de *benware*, é similar às buscas *online* e que, não permitindo a lei a realização de buscas *online*, também a vigilância nas fontes não é permitida. Contudo, como veremos, as buscas *online* são admissíveis à luz da lei portuguesa e, para além disso, a vigilância nas fontes e as buscas *online* são realidades completamente diversas, pois aquela

constitui uma intervenção nas comunicações, ao passo que esta consiste no rastreio do sistema informático na sua globalidade.

Em quinto lugar, poderia aduzir-se que, se o legislador alemão sentiu necessidade de regular expressamente a vigilância nas fontes, então, a sua não previsão legal expressa torna-a inadmissível à luz do Direito português. Todavia, sem prejuízo de ser preferível uma previsão legal expressa, consideramos que a nossa lei vigente contém suficientes salvaguardas em termos de restrição de direitos fundamentais; e também não podemos olvidar que as normas relativas aos meios de obtenção de prova não são normas processuais penais materiais (e não devem, por isso, seguir o mesmo regime das normas penais positivas)[92] nem que as exigências de certeza jurídica e de tutela da confiança[93] não são as mesmas quando se trate de impor limitações à licitude de condutas e quando se estabelecem os requisitos da utilização de um dado meio de obtenção de prova[94].

E, por último, nem se diga que, como aduzem COSTA ANDRADE e o *Bundesverfassungsgericht*[95], implicando a execução da vigilância nas fontes a prévia instalação de *malware* (para nós, *benware*), não está garantido o não acesso a outras informações (*v.g.* dados armazenados, navegação na Internet, etc.) para além das comunicações por VoIP. Com efeito, ainda que, em abstrato, tal pudesse suceder, não há que partir de uma suspeição generalizada quanto à atuação das autoridades e, se se concluísse que assim sucedera, as provas seriam ilícitas e as pessoas que assim atuassem seriam alvo de responsabilidade penal, civil e disciplinar.

Em suma, a vigilância nas fontes é admissível à luz do art. 18.º da Lei n.º 109/2009. No entanto, para afastar quaisquer dúvidas a este respeito, o legislador português deveria, tal como fez o legislador alemão, prever expressamente a possibilidade de lançar mão da vigilância nas fontes. E afirmamos que o legislador deverá prever expressamente essa possibilidade, atenta a elevada utilização das comunicações por VoIP nos dias de hoje e a

92 *Vide* os nossos argumentos em DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 298-299.
93 Como refere LARENZ, Metodologia da Ciência do Direito, 3.ª Edição, pp. 603-604, nem toda a confiança merecerá proteção, apenas a merecendo aquela que for justificada pelas circunstâncias e sendo que o princípio da confiança poderá colidir com outros princípios jurídicos a que poderá caber a prevalência no caso concreto.
94 Cfr. Acórdão Malone c. Reino Unido, do Tribunal Europeu dos Direitos Humanos e Sentença do *Tribunal Constitucional de España* n.º 49/1999.
Quanto às razões por que entendemos que as exigências de certeza jurídica e de tutela da confiança não são as mesmas em ambas as situações, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 290-291.
95 COSTA ANDRADE, "Bruscamente no Verão Passado" p. 165, e Sentença do *Bundesverfassungsgericht* de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07).

existência de aplicações informáticas que proporcionam uma elevadíssima proteção às comunicações realizadas com recurso a essas aplicações (*máxime* o *Telegram*), que torna as comunicações por VoIP um dos meios preferidos dos criminosos para a preparação e execução dos crimes e apagamento dos seus vestígios e, desse modo, a interceção de tais comunicações é absolutamente essencial para a descoberta da verdade material e para a obtenção de provas do cometimento de crimes[96].

Passando às buscas *online*, sendo a nossa lei omissa também quanto a este meio de obtenção de prova, não existe acordo na Doutrina quanto à sua admissibilidade[97] e, entre os defensores da admissibilidade, não existe acordo quanto à norma habilitante[98]. A este respeito, entendemos que a análise deverá partir da diferenciação entre os casos em que a busca consiste num único acesso (*Daten-Spiegelung*) e os casos em que ocorre de forma contínua e prolongada no tempo (*Daten-Monitoring*).

Começando pelos casos de *Daten-Spiegelung*, prevê-se, no art. 15.º da Lei n.º 109/2009, a possibilidade de realizar pesquisas de dados informáticos armazenados em sistemas

96 Como se viu no recente Caso EncroChat. A respeito deste caso, *vide* EUROPOL, "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" (Press release).

97 PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 545, JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 42 e ss. (embora apenas no âmbito de uma ação encoberta em ambiente informático-digital), e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 809 e ss., e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 226 e ss., pronunciam-se pela admissibilidade, ao passo que DAVID SILVA RAMALHO, "O uso de *Malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, p. 227, e também em Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 346 e ss., RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, pp. 196 e ss., 248 e 273, BENJAMIM SILVA RODRIGUES, Da Prova Penal, II, pp. 474-475, ARMANDO DIAS RAMOS, A prova digital em processo penal: O correio eletrónico, p. 91, MARIA BEATRIZ SEABRA DE BRITO, Novas Tecnologias e Legalidade da prova em Processo Penal, p. 97, e MARCOLINO DE JESUS, Os Meios de Obtenção de Prova em Processo Penal, p. 196, se pronunciam no sentido oposto.

DAVID SILVA RAMALHO, "O uso de m*alware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, n.º 16, p. 227, e também em Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 346 e ss., entende 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*.

98 Ao passo que PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 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 é 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), JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 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, como veremos, concordamos com PAULO PINTO DE ALBUQUERQUE, embora com as especificidades que referiremos no texto e que sempre temos defendido noutras publicações.

informáticos, não exigindo a lei que a pesquisa apenas possa ser "presencial", "física" (porquanto se refere apenas à obtenção de dados informáticos armazenados num sistema informático e não ao modo concreto da sua obtenção). Por isso, em obediência ao princípio *ubi lex non distinguit nec nos distinguere debemus*, a busca *online* na modalidade de *Daten-Spiegelung* poderá ser realizada com base neste preceito.

Passando aos casos de *Daten-Monitoring*, que, ao permitir uma monitorização, em tempo real e prolongada no tempo, dos dados existentes num sistema informático e da própria navegação *online*, possui uma danosidade muito similar à da intervenção nas comunicações eletrónicas em termos de restrição de direitos fundamentais. Na medida em que o legislador, ao admitir as buscas *online* no art. 15.º da Lei n.º 109/2009, não opera qualquer distinção, consideramos que tal preceito permite, também na modalidade de *Daten-Monitoring*, a realização de buscas *online*. Porém, atenta a sua maior danosidade face à modalidade de *Daten-Spiegelung* e sendo essa danosidade similar à da intervenção nas comunicações eletrónicas, deverá operar-se uma interpretação conforme à Constituição (por imposição da proibição do excesso), pelo que o art. 15.º deverá ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* na modalidade de *Daten-Monitoring* nos casos em que também fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art. 18.º da Lei n.º 109/2009, aplicando-se *mutatis mutandis* o respetivo regime jurídico.

Contra a admissibilidade das buscas *online* à luz do Direito português são pensáveis, em abstrato, os seguintes argumentos:

a) o facto de a lei exigir a presença da autoridade judiciária durante a pesquisa de dados informáticos (cf.. art. 15.º, n.º 1, da Lei n.º 109/2009);

b) a circunstância de o art. 15.º, n.º 6, da Lei n.º 109/2009 mandar aplicar as regras de execução das buscas previstas no CPP e no Estatuto do Jornalista (entre as quais se conta a entrega, ao visado, de uma cópia do despacho que determinou a busca e a possibilidade de assistir à diligência e fazer-se acompanhar por um terceiro);

c) as formas de efetivar a apreensão dos dados previstas no art. 16.º, n.º 7, als. a) a d), da Lei n.º 109/2009; e

d) a lei não prever expressamente as buscas *online*.

Contudo, quanto à necessidade de presença da autoridade judiciária durante a pesquisa de dados informáticos, além de se tratar de uma regra de cariz meramente procedimental, o próprio legislador refere que tal dever só existirá "*sempre que* [for] *possível*", pelo que a não

presença em nada obsta à admissibilidade da busca *online*[99]; ademais, a presença do magistrado, porque a lei não o especifica (e, como tal, não impõe qualquer distinção entre ambas as situações), tanto poderá ser para dirigir *in loco* a diligência como para o fazer *online*, não impondo a lei que esteja no local onde está o sistema informático visado, pelo que poderá estar no local onde está o sistema informático através do qual se acede[100].

Quanto à circunstância de, no art. 15.º, n.º 6, da Lei n.º 109/2009, o legislador mandar aplicar as regras das buscas "*com as necessárias adaptações*", esse preceito não exige que a busca informática seja "presencial" (pois o conceito de busca deverá ser lido de forma atualista, daí resultando que não tem de ser necessariamente realizada de forma "aberta" e "presencial" nem tem de se limitar à apreensão de coisas corpóreas, podendo e devendo ser dirigidas à descoberta de quaisquer meios de prova e de vestígios do crime – que é a finalidade de qualquer busca –, sejam corpóreos ou não[101]); além disso, as regras relativas às buscas que aqui estão em causa são de cariz procedimental e não material (ou seja, referem-se ao "como" e não ao "se")[102].

No que concerne às formas de efetivar a apreensão dos dados previstas no art. 16.º, n.º 7, als. a) a d), da Lei n.º 109/2009, a lei não impõe que a apreensão dos dados informáticos ocorra no local onde o sistema informático ou o suporte em que estão armazenados se encontram (não se podendo olvidar que a sua efetiva localização pode nem ser conhecida das autoridades[103] ou situar-se num Estado que recusa qualquer cooperação internacional), podendo ser concretizada à distância mediante cópia em suporte autónomo[104], sendo que, pelo

99 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 809-810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 228, e, à luz do Direito alemão, Sentença do *Bundesgerichtshof* de 21 de fevereiro de 2006. Relativamente às buscas não domiciliárias e às buscas domiciliárias, como refere DUARTE RODRIGUES NUNES, Revistas e buscas no Código de Processo Penal, pp. 93 e 163, a não observância do art. 174.º, n.º 3, do CPP constitui uma mera irregularidade que não afeta a validade das provas obtidas (cfr. arts. 118.º, n.ºs 1 e 2, e 123.º do CPP).

100 Cfr. JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 42 (nota 29), e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 228-229.

101 Cfr. KEMPER, "Die Beschlagnahmefähigkeit von Daten und E-Mails", *in* Neue Zeitschrift für Strafrecht, 2005, pp. 538-539, HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 123, e Sentença do *Bundesgerichtshof* de 21 de fevereiro de 2006.

102 Cfr., à luz do Direito alemão, Sentença do *Bundesgerichtshof* de 21 de fevereiro de 2006.

103 A utilização de *proxies* permite simular que o sistema informático se encontra num país diverso e até muito distante do país onde realmente se encontra e, desse modo, dissimular a verdadeira localização. Do mesmo modo, no caso do *Cloud computing*, a localização dos servidores onde os dados estão armazenados pode não ser conhecida.

104 Cfr. JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 42 (nota 29), e DUARTE RODRIGUES NUNES, O problema da admissibilidade

menos no caso das formas de apreensão previstas nas als. b) e d), do ponto de vista técnico, a apreensão pode perfeitamente ser efetivada *online* e, nos termos do corpo do n.º 7 do art. 16.º, o legislador determina que a escolha da forma de concretizar a apreensão deverá nortear-se por critérios de adequação e de proporcionalidade[105]; ademais, nos casos previstos no art. 15.º, n.º 5 (que, na Alemanha, é designada por "*busca online light*"), a apreensão dos dados só poderá ser efetuada *online*, dúvidas não restando de que, nesses casos – expressamente previstos na lei –, a circunstância de a apreensão dos dados só poder ser efetuada *online*, não impede a realização de pesquisas em sistemas informáticos[106].

E, quanto ao argumento da falta de previsão legal, em primeiro lugar, a lei não distingue entre pesquisas "presenciais" e pesquisas *online*, não exclui expressamente as pesquisas *online* nem restringe as pesquisas em sistemas informáticos apenas aos casos em que sejam "presenciais"; e, além disso, prevê, inclusivamente, um caso de pesquisa remota no art. 15.º, n.º 5 da Lei n.º 109/2009.

Em segundo lugar, em 2009 já era tecnicamente possível a realização de pesquisas remotas em sistemas informáticos (ao ponto de o legislador ter previsto uma modalidade – que não configura uma busca *online* na aceção que aqui estamos a analisar – de pesquisa em sistema informático como a que consta do art. 15.º, n.º 5 da Lei n.º 109/2009), pelo que não se pode considerar – à míngua de elementos que apontem no sentido oposto – que o legislador apenas terá tido em conta as pesquisas "presenciais".

Em terceiro lugar, a busca *online* nem sequer implica a entrada no local onde está o sistema informático (que até poderá ser um espaço que goza da tutela do direito à inviolabilidade do domicílio) nem a apreensão do sistema informático[107], pelo que, nos casos em que a busca *online* consista num único acesso, é menos lesiva do que uma pesquisa "presencial" em termos de restrição de direitos fundamentais[108].

---

dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 229.

105 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 810, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 229.

106 Assim, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 810-811, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 229.

107 Cfr. HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 124.

108 No mesmo sentido, SUSAN BRENNER, Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, p. 9; contra, DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 755, LORENA BACHMAIER WINTER, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, pp. 24-25, e Sentença Riley *v.* California do *Supreme Court of the United States* (2014).

Em quarto lugar, o art. 15.º da Lei n.º 109/2009[109] prevê um caso de pesquisa em sistema informático realizado remotamente, pelo que, tendo em conta o que referimos no primeiro argumento, podemos fundar a admissibilidade da busca *online*, pelo menos numa interpretação extensiva[110] desse preceito. Na verdade, radicando a particularidade da busca *online* em não ser realizada no local onde se encontra o sistema informático visado, a busca *online* nem por isso deixa de ser uma pesquisa de dados informáticos específicos e determinados que estão armazenados num determinado sistema informático, pelo que continuamos no âmbito do sentido possível da expressão "*pesquisa de dados informáticos específicos e determinados que estão armazenados num determinado sistema informático*".

Em quinto lugar, nem se diga que, em termos de pesquisa *online*, o legislador ao prever a extensão *online* da pesquisa no art. 15.º, n.º 5, da Lei n.º 109/2009 apenas quis permitir essa extensão e nada mais, porquanto tal extensão também poderá ocorrer no âmbito de uma busca *online*, designadamente quando, no decurso da mesma, se verifique que os dados estão (ou existem mais dados relevantes) armazenados num outro sistema informático que seja legitimamente acessível através do sistema que estava a ser alvo da busca *online*.

Em sexto lugar, a busca *online* é apenas uma forma de efetivação de uma pesquisa num sistema informático, sendo que nada na Constituição ou na lei impõe que as diligências investigatórias sejam realizadas, em regra, com o conhecimento dos visados, razão pela qual, o mero caráter "oculto" não é argumento para obstar à admissibilidade das buscas *online*[111].

Em sétimo lugar, a especificidade da busca *online* que mais dúvidas suscita quanto à sua admissibilidade é a prévia instalação de programas informáticos que permitam o acesso (necessariamente sub-reptício) ao sistema informático. Ora, a instalação de *benware* é um mero ato preparatório da pesquisa informática (na modalidade de busca *online*), à semelhança do que sucede com essa mesma instalação no caso da vigilância nas fontes, com a colocação de localizadores de GPS no caso da obtenção de dados de localização através de sistema GPS ou com a duplicação da linha do número do telefone visado pela escuta telefónica.

Em oitavo lugar, ainda que a mera instalação do *benware* restrinja direitos fundamentais, trata-se de uma restrição muito pouco significativa (sobretudo quando comparada com a restrição que pode resultar do acesso aos dados informáticos, tudo

109 Cfr. PAULO PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 502 e 545.

110 E não atualista, dado que, em 2009, já era tecnicamente possível efetuar buscas *online*. Porém, na medida em que, não distinguindo a lei entre pesquisa "presencial" e busca *online*, cremos que nem será necessário lançar mão de uma interpretação extensiva.

111 Cfr. HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 123.

dependendo da natureza dos mesmos) e, para além disso, como referimos, nos casos em que a busca *online* consista num único acesso, é menos lesiva do que a restrição decorrente de uma pesquisa "presencial".

Em nono lugar, nem se diga que, como aduzem COSTA ANDRADE e o *Bundesverfassungsgericht*[112], implicando a execução da busca *online* a prévia instalação de *malware* (para nós, *benware*), não está garantido o não acesso a outras informações (*v.g.* ao teor de comunicações através de vigilância nas fontes não autorizada), pois, como referimos supra, não podemos partir de uma suspeição generalizada quanto à atuação das autoridades e, se se concluísse que assim teria acontecido, as provas seriam ilícitas e as pessoas que assim atuassem seriam alvo de responsabilidade penal, civil e disciplinar.

E, em décimo lugar, poderia aduzir-se que, se os legisladores alemão e espanhol sentiram necessidade de regular expressamente as buscas *online*, então, pelo menos no caso das buscas *online* na modalidade de *Daten-Monitoring*, a não previsão legal expressa torna as buscas *online* inadmissíveis à luz do Direito português. Todavia, sem prejuízo de entendermos que será preferível que o legislador luso preveja e regule expressamente este meio de obtenção de prova, consideramos que a nossa lei vigente contém suficientes salvaguardas em termos de restrição de direitos fundamentais (designadamente se se adotar um regime jurídico como o que propugnamos[113]), não se podendo olvidar que as normas relativas aos meios de obtenção de prova não são normas processuais penais materiais (e não devem, por isso, seguir o mesmo regime das normas penais positivas)[114] nem que as exigências de certeza jurídica e de tutela da confiança[115] não são as mesmas quando se trate de impor limitações à licitude de condutas e quando se estabelecem os requisitos da utilização de um dado meio de obtenção de prova[116].

---

112 COSTA ANDRADE, "Bruscamente no Verão Passado" p. 165, e Sentença do *Bundesverfassungsgericht* de 27/02/2008 (1 BvR 370/07 e 1 BvR 595/07).

113 *Vide*, a este respeito, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 809 e ss., e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 231 e ss.

114 *Vide* os nossos argumentos em DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 298-299.

115 Como refere LARENZ, Metodologia da Ciência do Direito, 3.ª Edição, pp. 603-604, nem toda a confiança merecerá proteção, apenas a merecendo a confiança que for justificada pelas circunstâncias e sendo que o princípio da confiança poderá colidir com outros princípios jurídicos a que poderá caber a prevalência no caso concreto.

116 Cfr. Acórdão Malone c. Reino Unido, do Tribunal Europeu dos Direitos Humanos e Sentença do *Tribunal Constitucional de España* n.º 49/1999.

Quanto às razões por que entendemos que as exigências de certeza jurídica e de tutela da confiança não são as mesmas em ambas as situações, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 290-291.

Deste modo, entendemos que a busca *online* é admissível entre nós, à luz do art. 15.º da Lei n.º 109/2009, embora, nos casos de *Daten-Monitoring*, por imposição da proibição do excesso, o art. 15.º deva ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* nos casos em que também fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art. 18.º da Lei n.º 109/2009, aplicando-se *mutatis mutandis* o respetivo regime jurídico.

No entanto, reiteramos que, para afastar quaisquer dúvidas a este respeito, o legislador português devesse, tal como fizeram os legisladores espanhol e alemão, prever expressamente a possibilidade de lançar mão das buscas *online*.

E entendemos que a solução legal só poderá ser no sentido da admissibilidade do recurso às buscas *online*, pois, em primeiro lugar, a busca *online* é um meio extremamente eficaz e necessário para a investigação criminal «*tendo em conta a presença praticamente ubíqua do computador no quotidiano dos cidadãos em todos os sectores e domínios da vida e, portanto, também do lado da preparação, planificação e gestão de meios e recursos do crime. E tanto mais quanto mais a fenomenologia criminal ganhar em mobilidade, racionalidade e organização. Resumidamente (…) também as manifestações mais insidiosas e perigosas da criminalidade organizada, e concretamente o terrorismo, apresentam hoje uma indissociável associação à informática. E, nessa medida, expõem uma extensa e fecunda superfície à investigação das instâncias de controlo. E é assim, mesmo tendo em conta os obstáculos técnicos ainda subsistentes e o recurso cada vez mais generalizado a programas de proteção e "blindagem" dos dados*»[117].

Em segundo lugar, a busca *online* permite monitorizar a navegação na Internet[118], que, não constituindo um processo comunicacional, não pode ser objeto de intervenções nas comunicações. Ademais, em face da existência da *Dark Web*, a determinação do sistema onde os dados estão armazenados ou de onde poderão ser acedidos e a obtenção de credenciais de

117 COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 166-167; no mesmo sentido, JOÃO CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 44, HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 121, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 813, e também em Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 231-232, e DAVID SILVA RAMALHO, "The use of malware as a mean of obtaining evidence in Portuguese criminal proceedings", *in* Digital Evidence and Electronic Signature Law Review, 11 (2014), p. 55.

118 Cfr. HOLZNER, Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, p. 11, e BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 161.

acesso a *websites* não publicamente acessíveis ou a *darknets* poderá depender do recurso a métodos "ocultos" como as ações encobertas ou as buscas *online*[119].

Em terceiro lugar, a busca *online*, além de permitir – por via do *keylogging* – a obtenção de *passwords* e de outros mecanismos afins[120], permite também analisar o sistema informático em funcionamento e, desse modo, superar as dificuldades causadas pela utilização de medidas antiforenses e aceder mais fácil e rapidamente à informação, o que a pesquisa "presencial" não permite[121], bem como tem, face às pesquisas "presenciais", a vantagem de, pelo seu caráter "oculto", não "revelar" aos visados que estão a ser alvo de uma investigação e de recolha de provas, com evidentes ganhos em termos de eficácia[122].

Em quarto lugar, a busca *online* permite aceder a outros suportes informáticos que não estejam na proximidade do sistema informático no momento em que a pesquisa "presencial" é realizada e cuja existência seja desconhecida pelas autoridades ou lhes tenha sido omitida, bem como, nos casos de *Daten-Monitoring*, permite apreender ficheiros informáticos que apenas estão no sistema informático por um breve lapso de tempo antes de serem apagados[123].

119 Cfr. DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", *in* Revista de Concorrência e Regulação n.ºs 14/15, p. 402.
120 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 161, e DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", *in* Revista de Concorrência e Regulação n.ºs 14/15, p. 402.
121 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, pp. 158 e ss., DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 745, e DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", *in* Revista de Concorrência e Regulação n.ºs 14/15, p. 402.
122 Cfr. ROGGAN, "Präventive Online-Durchsuchungen", *in* Online-Durchsuchungen, p. 99, e BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 158.
123 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, pp. 159 e 161.

Em quinto lugar, a busca *online* permite investigar os ataques de DDoS[124] lançados através do uso de *botnets*[125].

Por fim, a busca *online* poderá ser um meio de suprir as insuficiências da intervenção nas comunicações eletrónicas ao permitir a obtenção de informação cuja consecução não tenha sido possível durante o processo comunicacional e que tenha sido armazenada num sistema informático – incluindo no caso do *Cloud computing*[126] – cuja localização física não tenha sido possível determinar[127] (o que impede, *ab initio*, a solicitação de cooperação judiciária internacional[128]) ou que estejam localizados no Estrangeiro[129] (especialmente quando se trate de países qualificáveis como paraísos fiscais e/ou jurídico-penais, em que as autoridades locais não cooperam com as suas congéneres de outros países em matéria de investigação criminal ou em que essa cooperação é extremamente demorada e com perdas irreparáveis no plano probatório), superando assim as insuficiências da interceção de

124 O ataque do tipo *DoS* (*Denial of Service*), também designado por ataque de negação de serviço, consiste na provocação de uma sobrecarga num sistema informático para que os recursos desse sistema fiquem indisponíveis para os seus utilizadores. Para executar um ataque deste tipo, o atacante envia diversos pedidos de pacotes para o alvo para que ele fique tão sobrecarregado que não consiga responder a qualquer outro pedido de pacote, deixando os seus utilizadores de poder aceder aos dados que se encontram nesse sistema; outra forma de execução consiste em o atacante forçar a vítima a reinicializar ou a consumir todos os recursos da memória e de processamento ou de outro *hardware*, para que o sistema informático não possa fornecer o serviço. Este ataque do tipo *DoS* não constitui qualquer invasão do sistema (que apenas é incapacitado por via da sua sobrecarga), envolvendo apenas um atacante, sendo o mesmo sistema informático que faz os vários pedidos de pacotes ao alvo, apenas sendo atingidos servidores fracos e computadores com pouca capacidade técnica.

Por seu turno, o ataque do tipo *DDoS* (*Distributed Denial of Service*) consiste em um sistema informático "mestre" gerenciar um determinado número (podendo ser na ordem dos milhares) de sistemas informáticos (*zumbis*), que irão ser "escravizados" para acederem, conjunta e ininterruptamente, ao mesmo recurso de um dado sistema informático, a fim de o sobrecarregar e impedir os seus utilizadores de acederem a esse sistema (que, tanto pode ficar bloqueado como reiniciar constantemente, dependendo do recurso que foi atingido pelo ataque).

125 Cfr. DEVIN M. ADAMS, "The 2016 Amendment to Criminal Rule 41: National search warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), p. 745.

A *botnet* consiste numa rede de sistemas informáticos infetados por *bots* semelhantes. Os agentes do crime irão disseminar m*alware* num grande número de sistemas informáticos, com o objetivo de os transformar em *zumbis* (também designados por *Bots*), passando a executar, de forma automatizada e sem que o seu utilizador se aperceba, tarefas na Internet para fins de envio de *spam*, disseminação de vírus, de ataque a sistemas informáticos (incluindo atos de Ciberterrorismo), de cometimento de fraudes, etc. A criação de *botnets* constitui também um ato preparatório de ataques do tipo *DDoS*.

126 No Direito alemão, a pesquisa dos dados armazenados numa nuvem é operada ao abrigo do §100b, relativo à busca *online* (cfr. MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 422.

127 Cfr. ORTIZ PRADILLO, "El registro «*online*» de equipos informáticos como medida de investigación contra el terrorismo (*online durchsuchung*)", *in* Terrorismo y Estado de Derecho, p. 469, HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 121, e BÖCKENFÖRDE, Die Ermittlung im Netz, p. 469.

128 E, no caso do *Cloud computing*, até poderá saber-se em que nuvem os dados informáticos estão armazenados, mas desconhecer-se o país onde os servidores se encontram (o que impossibilita qualquer pedido de auxílio) ou, conhecendo-se o país, tratar-se de um país que não coopera em matéria de investigação criminal ou a cooperação é demasiado lenta e com perdas irreparáveis em termos de prova. Acerca da dificuldade da investigação em casos de *Cloud computing*, *vide* DAVID SILVA RAMALHO, "A recolha de prova penal em sistemas de computação em nuvem", *in* Revista de Direito Intelectual, 2014, n.º 2, *passim*.

129 Cfr. BÖCKENFÖRDE, Die Ermittlung im Netz, p. 221.

comunicações, uma vez que, em regra, os dados armazenados no sistema não são remetidos por correio eletrónico ou, sendo-o, são-no por via de encriptação do *e-mail*[130].

Por fim, quanto à vigilância acústica e ótica, como referimos, a nossa lei prevê dois meios de obtenção de prova distintos[131]: a interceção de comunicações entre presentes (art. 189.º, n.º 1, do CPP) e o registo de voz e imagem (art. 6.º da Lei n.º 5/2002)[132]. Todavia, tal como não previu expressamente a possibilidade de vigilância acústica e ótica no interior do domicílio (e de espaços que gozam da tutela constitucional do direito à inviolabilidade do domicílio)[133], o legislador também não previu a possibilidade de realizar vigilâncias acústicas e/ou óticas através da ativação da câmara e/ou do microfone de um sistema informático (com a prévia instalação do *software* necessário para esse efeito), como fez o legislador italiano relativamente ao *captatore informatico*.

Pela nossa parte, à semelhança do que referimos quanto à vigilância nas fontes e à busca *online*, entendemos que nada impede a realização de vigilâncias acústicas e/ou óticas através da ativação da câmara e/ou do microfone de um sistema informático precedida da instalação de *benware* (*captatore informatico*), pelo que tal possibilidade é admissível à luz do Direito português.

Em primeiro lugar, o *captatore informatico* consiste apenas num meio de execução das interceções de comunicações entre presentes ou do registo de voz e/ou imagem[134],

Em segundo lugar, a instalação do *benware* é um mero ato preparatório da vigilância acústica e/ou ótica que implica uma restrição de direitos fundamentais muito pouco significativa (sobretudo quando comparada com a restrição que resulta da execução da vigilância acústica e/ou ótica) e porventura menos intensa do que a restrição que resultaria da

130 Cfr. BUERMEYER, Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, p. 159, e HOFMANN, "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, p. 121.

131 Relativamente à nossa crítica a esta bipartição de meios de obtenção de prova e à preferibilidade de uma unificação de regimes jurídicos, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 682-683.

132 Acerca da diferença entre ambos os meios de obtenção de prova quanto ao seu âmbito de aplicação, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 680 e ss.

133 O que leva alguma Doutrina, a nosso ver sem razão, a pronunciar-se no sentido da inadmissibilidade da interceção de comunicações entre presentes e do registo de voz e imagem "domiciliários". Acerca das razões porque entendemos que interceção de comunicações entre presentes e do registo de voz e imagem no interior do domicílio e/ou de outros espaços que gozam da tutela constitucional do direito à inviolabilidade do domicílio é admissível à luz do Direito português, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 692 e ss.

134 Cfr., à luz do Direito italiano, Sentenças das *Sezioni Unite* da *Suprema Corte de Cassazione* de 28/04/2016-01/07/2016, n.º 26889, e da *Suprema Corte di Cassazione* de 30/05/2017-20/10/2017, n.º 48370 (Sez. V), 08/03/2018-09/10/2018, n.º 45486 (Sez. VI), e 25/06/2019-17/12/2019, n.º 50972 (Sez. I).

entrada dos agentes no local onde a vigilância deverá ocorrer (sobretudo se se tratar do domicílio) para colocarem os microfones e/ou as câmaras (que também constitui um mero ato preparatório da vigilância acústica e/ou ótica executadas desse modo).

Em terceiro lugar, os arts. 189.º, n.º 1, do CPP e 6.º da Lei n.º 5/2002 referem-se à "interceção de comunicações entre presentes" e ao "registo de voz e imagem, por qualquer meio, sem consentimento do visado", respetivamente. Ora, no caso do art. 189.º, n.º 1, do CPP, o legislador não consagra qualquer limitação ou restrição quanto ao modo de execução da interceção (pelo que *ubi lex non distinguit nec nos distinguere debemus*) e, no art. 6.º da Lei n.º 5/2002, vai ainda mais longe ao permitir expressamente o registo de voz e imagem *por qualquer meio* (onde se pode incluir o *captatore informatico*).

Em quarto lugar, o recurso ao *captatore informatico* dispensa a entrada "física" das autoridades nos locais reservados e não acessíveis ao público (incluindo o domicílio) em que fosse necessário instalar as câmaras e os microfones (sendo, por isso, como referimos, menos lesivo para os direitos fundamentais e envolvendo menos riscos para os agentes policiais).

Em quinto lugar, poderia aduzir-se que, se o legislador italiano sentiu necessidade de regular expressamente o *captatore informatico*, então, a sua não previsão legal expressa torna-o inadmissível à luz do Direito português[135]. Todavia, sem prejuízo de ser preferível uma previsão legal expressa, consideramos que a nossa lei vigente contém suficientes salvaguardas em termos de restrição de direitos fundamentais; e também não podemos olvidar que as normas relativas aos meios de obtenção de prova não são normas processuais penais materiais (e não devem, por isso, seguir o mesmo regime das normas penais positivas)[136] nem que as exigências de certeza jurídica e de tutela da confiança[137] não são as mesmas quando se trate de impor limitações à licitude de condutas e quando se estabelecem os requisitos da utilização de um dado meio de obtenção de prova[138].

---

135 Como entende MARCUS KÖHLER, "100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, p. 421, precisamente por essa razão. à luz do Direito alemão.

136 *Vide* os nossos argumentos em DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 298-299.

137 Como refere LARENZ, Metodologia da Ciência do Direito, 3.ª Edição, pp. 603-604, nem toda a confiança merecerá proteção, apenas a merecendo aquela que seja justificada pelas circunstâncias; ademais, o princípio da confiança pode colidir com outros princípios que devam prevalecer no caso concreto.

138 Cfr. Acórdão Malone c. Reino Unido, do Tribunal Europeu dos Direitos Humanos e Sentença do *Tribunal Constitucional de España* n.º 49/1999.

Quanto às razões por que entendemos que as exigências de certeza jurídica e de tutela da confiança não são as mesmas em ambas as situações, *vide* DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 290-291.

E, por último, poderia também aduzir-se – como se aduz quanto à vigilância nas fontes e à busca *online* – que, implicando a utilização do *captatore informatico* a prévia instalação de *malware* (para nós, *benware*), não está garantido o não acesso a outras informações (*v.g.* dados armazenados, navegação na Internet, comunicações eletrónicas, etc.). Contudo, como referimos supra, não podemos partir de uma suspeição generalizada quanto à atuação das autoridades e, se se concluísse que assim sucedera, as provas seriam ilícitas e as pessoas que assim atuassem seriam alvo de responsabilidade penal, civil e disciplinar.

Assim, consideramos que a vigilância acústica e/ou ótica através da ativação da câmara e/ou do microfone de um sistema informático precedidas da instalação de *benware* (*captatore informatico*) é admissível à luz do Direito português, mais concretamente nos termos dos arts. 189.º, n.º 1, do CPP e 6.º da Lei n.º 5/2002.

Contudo, o legislador português deveria seguir o exemplo do legislador italiano e prever expressamente a possibilidade de utilização do *captatore informatico*, a fim de dissipar quaisquer dúvidas que possam surgir a esse respeito. E, tal como entendemos nos casos da vigilância nas fontes e da busca *online*, no que tange à utilização do *captatore informatico*, a solução legal só poderá ser no sentido da sua admissibilidade.

Com efeito, sobretudo no caso de criminosos particularmente cautelosos (como sucede no âmbito da criminalidade organizada, terrorismo, criminalidade económico-financeira e Cibercrime), a realização de vigilância acústica e ótica em locais onde os criminosos se sentem especialmente seguros (*máxime* no seu domicílio) e que poderão utilizar para preparar ou executar crimes ou eliminar os vestígios da prática de crimes ou partilhar detalhes a esse respeito com pessoas da sua confiança (*máxime* familiares próximos, que também poderão fazer parte da organização) poderá ser essencial[139].

Ademais, em grupos criminosos "etnicamente fechados" ou assentes exclusivamente em laços familiares, as ações encobertas tendem a ser inúteis ou impossíveis de realizar[140] e, sabendo esses criminosos que as comunicações eletrónicas poderão ser acedidas pelas autoridades[141], tenderão a confiar mais na segurança que lhes é dada pelo domicílio do que na que lhes é oferecida por uma linha telefónica ou pelo Ciberespaço e, por isso, as

139 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 696.

140 Aludindo à utilidade da vigilância acústica no interior do domicílio como mecanismo para suprir as insuficiências das ações encobertas, *vide* KREY/HAUBRICH, "Zeugenschutz, Rasterfahndung, Lauschangriff, Verdeckte Ermittler", *in* Juristische Rundschau, 1992, p. 313.

141 E, como se afirma na Sentença do *Bundesverfassungsgericht* de 03/03/2004 (1 BvR 2378/98 e 1 BvR 1084/99), o recurso à intervenção nas comunicações eletrónicas, *maxime* as escutas telefónicas, apresenta uma outra desvantagem face à vigilância acústica: apenas permite intercetar as comunicações que são levadas a cabo mediante meios de comunicação à distância.

probabilidades de serem "surpreendidos" no interior do seu domicílio são muito maiores do que enquanto realizam comunicações eletrónicas, proporcionando informações que as autoridades dificilmente obteriam de outra forma[142].

E a vigilância acústica e ótica no interior do domicílio são métodos "ocultos" que permitem atingir eficazmente as cúpulas das organizações criminosas, revelando a sua estrutura organizatória e permitindo identificar os líderes, os apoiantes, os financiadores e os colaboradores externos[143], sendo a sua identificação e prisão essencial para desmantelar a organização e impedir a continuação da sua atividade.

E também não podemos olvidar que a vigilância acústica e ótica apresentam diversas e importantes vantagens face à vigilância "física": (1) permitem a recolha de som e imagem sem necessidade de os investigadores estarem nesse local, (2) não levantam suspeitas de estarem a ser recolhidas provas da atividade criminosa, (3) não põem os investigadores em perigo e (4) proporcionam a obtenção de informações em locais onde não seria possível colocar agentes policiais sem levantar suspeitas[144]. E a vigilância ótica permite captar aspetos que poderão não ser captados pela vigilância acústica, por não conterem qualquer elemento sonoro (*v.g.* a mera entrega de dinheiro ao funcionário corrompido) ou ser usada linguagem codificada indecifrável na comunicação[145].

E especificamente quanto à utilização do *captatore informatico* no âmbito da vigilância acústica e ótica, pela natureza "itinerante" dos sistemas informáticos da atualidade (*smartphone*, *tablet*, computador), os sistemas informáticos podem ser utilizados, pelas autoridades como instrumentos de execução dessas vigilâncias[146], o que dispensa, tanto a entrada dos agentes da autoridade no local onde será realizada a vigilância acústica e/ou ótica para colocarem microfones ou câmaras como a sua permanência nas imediações desse local

142 Cfr. DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, pp. 696-697 (com referências bibliográficas e jurisprudenciais adicionais).

143 Assim, DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 697, e Sentença do *Bundesverfassungsgericht* de 03/03/2004 (1 BvR 2378/98 e 1 BvR 1084/99).

144 Cfr. MONTOYA, Informantes y Técnicas de Investigación Encubiertas, Análisis Constitucional y Procesal Penal, 2.ª Edição, p. 343, LEPSIUS, "Die Grenzen der präventivpolizeilichen Telefonüberwachung", *in* Juristische Ausbildung, 2005, p. 433, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 699.

145 Cfr. GARY MARX, Undercover, p. 58, e DUARTE RODRIGUES NUNES, O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, p. 700.

146 Cfr. Sentenças das *Sezioni Unite* da *Suprema Corte de Cassazione* de 28/04/2016-01/07/2016, n.º 26889, e da *Suprema Corte di Cassazione* de 30/05/2017-20/10/2017, n.º 48370 (Sez. V), 08/03/2018-09/10/2018, n.º 45486 (Sez. VI), e 25/06/2019-17/12/2019, n.º 50972 (Sez. I).

com os dispositivos necessários para a execução da vigilância a partir do exterior, com evidentes ganhos em termos de eficácia da medida e até de segurança dos próprios agentes.

Deste modo, consideramos que a utilização de *benware* no âmbito da investigação criminal é admissível à luz do Direito português vigente, embora – porque, como referimos, restringe o direito fundamental à confidencialidade e à integridade dos sistemas técnico-informacionais – fosse preferível que o legislador o previsse expressamente, a fim de afastar quaisquer dúvidas quanto a essa admissibilidade, que poderão gerar graves prejuízos em termos de eficácia da investigação e, consequentemente, graves deficiências ao nível da proteção dos direitos fundamentais dos cidadãos face a formas de criminalidade particularmente nocivas e que também atentam contra a própria subsistência do Estado de Direito (*máxime* no caso das Máfias, do terrorismo e da corrupção).

4. CONCLUSÕES

A) A crescente utilização das medidas antiforenses e de meios de comunicação como as comunicações por VoIP pelos criminosos dificulta de sobremaneira a deteção da prática de crimes, a descoberta da verdade material e a obtenção de provas.

B) Por isso, as autoridades necessitam cada vez mais de utilizar mecanismos/dispositivos que neutralizem as dificuldades decorrentes da utilização de medidas antiforenses e de meios de comunicação como as comunicações por VoIP pelos criminosos.

C) Um desses mecanismos/dispositivos é a instalação sub-reptícia de programas informáticos (vírus, *worms*, "cavalos de Troia", *keyloggers*, *backdoors*, *spyware*, etc.) que permitam que as autoridades se infiltrem num sistema informático alheio para obterem informações relevantes para a investigação (*benware*).

D) Pela necessária "clandestinidade" da instalação do *benware* nos sistemas informáticos visados – que faz antever o cariz "oculto" das medidas investigatórias cuja execução a sua instalação visa permitir –, a utilização do *benware* está intimamente ligada à questão dos métodos "ocultos" de investigação criminal.

E) A utilização de *benware* é essencial na busca *online* (*online-Durchsuchung*), na vigilância nas fontes (*Quellen-Telekommunikationsüberwachung* ou *Quellen-TKü*) e na vigilância acústica e/ou ótica (sob a forma de registo de voz e imagem ou de interceção de comunicações entre presentes) quando seja realizada mediante a ativação (sub-reptícia) da câmara e/ou do microfone do sistema informático (*captatore informatico*).

F) A utilização de *benware* restringe o direito fundamental à confidencialidade e à integridade dos sistemas técnico-informacionais.

G) Ao contrário de outras ordens jurídicas, o legislador português não regula expressamente a utilização de *benware*, o mesmo sucedendo com as buscas *online*, a vigilância nas fontes e a ativação sub-reptícia da câmara e/ou do microfone do sistema informático no âmbito do registo de voz e imagem ou da interceção de comunicações entre presentes, apenas existindo uma referência implícita ao uso de *benware* no art. 19.º, n.º 2, da Lei n.º 109/2009, em que se prevê a possibilidade de utilizar meios e dispositivos informáticos no âmbito das ações encobertas em ambiente informático-digital ou *online*.

H) Apesar disso, a vigilância nas fontes é admissível à luz do art. 18.º da Lei n.º 109/2009.

I) A busca *online* é admissível à luz do art. 15.º da Lei n.º 109/2009, embora, nos casos em que a infiltração no sistema informático seja levada a cabo de forma contínua e prolongada no tempo (*Daten-Monitoring*), o art. 15.º deva ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* nos casos em que também fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art. 18.º da Lei n.º 109/2009, aplicando-se *mutatis mutandis* o respetivo regime jurídico.

J) A vigilância acústica [sob a forma de a interceção de comunicações entre presentes (art. 189.º, n.º 1, do CPP) ou de registo de voz (art. 6.º da Lei n.º 5/2002)] e a vigilância ótica (registo de imagem, nos termos do art. 6.º da Lei n.º 5/2002) mediante a ativação sub-reptícia da câmara e/ou do microfone do sistema informático são admissíveis à luz dos mencionados normativos.

K) A utilização de *benware* no âmbito da investigação criminal é admissível à luz do Direito português vigente, embora fosse preferível que o legislador previsse essa possibilidade, a fim de afastar quaisquer dúvidas a este respeito.

BIBLIOGRAFIA

Adams, Devin M. – "The 2016 Amendment to Criminal Rule 41: National seach warrants to seize Cyberspace, "particularly" speaking", *in* University of Richmond Law Review, Volume 51 (2017), pp. 727 e ss., *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3335987* (consultado em 14/07/2020).

Albuquerque, Paulo Pinto de – Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, 4.ª Edição, Lisboa, 2011.

Andrade, Manuel da Costa – "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, Coimbra, 2009.

Andrade, Manuel da Costa – "Art. 194º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, 2.ª Edição, pp. 1080 e ss., Coimbra Editora, Coimbra, 2012.

Bachmaier Winter, Lorena – "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in* Boletín del Ministerio de Justicia, Núm. 2195, *in https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428206148*

?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheade

rname2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1701_Estudio.pdf&blobheadervalue2=1288794492107 (consultado em 13/07/2020).

Bär, Wolfgang – TK-Überwachung, §§100a-101 StPO mit Nebengesetzen Kommentar, Carl Heymanns Verlag, Colónia e Munique, 2010.

Baxter, Teri Dobbins – "Great (and Reasonable) Expectations: Fourth Amendment Protection for Attorney-Client Communications", *in* Seattle University Law Review 35, pp. 35 e ss., *in https://ssrn.com/abstract=1336980* (consultado em 14/07/2020).

Brenner, Susan – Fourth Amendment Future: Remote Computer Searches and The Use of Virtual Force, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1950703* (consultado em 14/07/2020).

Brenner Susan – "Law, Dissonance and Remote Computer Searches", *in* North Carolina Journal of Law & Technology, Volume 14, Issue 1, pp. 43 e ss., *in https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1238&context=ncjolt* (consultado em 14/07/2020).

Brito, **Maria Beatriz Seabra de** – Novas Tecnologias e Legalidade da prova em Processo Penal, Almedina, Coimbra, 2018.

Böckenförde, Thomas – Die Ermittlung im Netz, Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Mohr Siebeck, Tübingen, 2003.

Buermeyer, Ulf – Die "Online-Durchsuchung". Technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, *in http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8*, pp. 154 e ss. (consultado em 21/02/2011).

Buermeyer, Ulf/Bäcker, Matthias – Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO, *in http://www.hrr-strafrecht.de/hrr/archiv/09-10/index.php?sz=8*, pp. 329 e ss. (consultado em 11/11/2014).

Clancy, Thomas K. – "The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer", *in* Mississippi Law Journal, Vol. 75, pp. 193 e ss., *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1602052* (consultado em 14/07/2020).

Correia, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 29 e ss., Lisboa, 2014.

Díaz, Shelly Mott, "A Guilty Attorney with Innocent Clients: Invocation of the Fourth Amendment to Challenge the Search of Privileged Information", *in* Mississippi Law Journal, Volume 79, pp. 56 e ss., *in https://studylib.net/doc/8201263/invocation-of-the-fourth-amendment-to-challenge-the-* (consultado em 14/07/2020).

Europol – "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" (Press release), *in https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe* (consultado em 20/07/2020).

Hofmann, Manfred – "Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmassnahme?", *in* Neue Zeitschrift für Strafrecht, 2005, pp. 121 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2005.

Hoffmann-Riem, Wolfgang – Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigener informationstechnischer Systeme, *in www.jura.uni-hamburg.de/public/personen/hoffmann-riem/8.pdf* (consultado em 21/11/2014).

Holzner, Stefan – Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, Centaurus Verlag, Kenzingen, 2009.

Jesus, Francisco Marcolino de – Os Meios de Obtenção de Prova em Processo Penal, Almedina, Coimbra, 2011.

Kemper, Martin – "Die Beschlagnahmefähigkeit von Daten und E-Mails", *in* Neue Zeitschrift für Strafrecht, 2005, pp. 538 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2005.

Klesczewski, Diethelm – "Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von Strafprozessualen Ermittlungseingriffen im Internet", *in* Zeitschrift für die gesamte Strafrechtswissenschaft, 2012, pp. 737 e ss., Walter de Gruyter, Berlim, 2012.

Köhler, Marcus – "§ 100a", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 403 e ss., C.H. Beck, Munique, 2019.

Köhler, Marcus – "§ 100b", *in* Lutz Meyer-Goßner/Bertram Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62.ª Edição, pp. 420 e ss., C.H. Beck, Munique, 2019.

Krey, Volker/Haubrich, Edgar – "Zeugenschutz, Rasterfahndung, Lauschangriff, Verdeckte Ermittler", *in* Juristische Rundschau, 1992, pp. 309 e ss., Walter de Gruyter, Berlim e Nova Iorque, 1992.

Larenz, Karl – Metodologia da Ciência do Direito, 3.ª Edição (tradução de José Lamego), Fundação Calouste Gulbenkian, Lisboa, 1997.

Lepsius, Oliver – "Die Grenzen der präventivpolizeilichen Telefonüberwachung", *in* Juristische Ausbildung, 2005, pp. 929 e ss., Walter de Gruyter, Berlim, 2005.

Marx, Gary T. – Undercover, Police Surveillance in America, University of California Press, Berkeley e Los Angeles, 1988.

Mayer, Jonathan – Constitutional Malware, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633247* (consultado em 16/07/2020).

McArthur, Eric D. – "The Search and Seizure of Privileged Attorney-Client Communications", *in* University of Chicago Law Review, Vol. 72, *in https://chicagounbound.uchicago.edu/uclrev/vol72/iss2/7* (consultado em 14/07/2020).

Montoya, Mario Daniel – Informantes y Técnicas de Investigación Encubiertas, Análisis Constitucional y Procesal Penal, 2.ª Edição, Ad hoc, Buenos Aires, 2001.

Nack, Armin – "§100a", *in* Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 6.ª Edição, pp. 471 e ss., Verlag C. H. Beck, Munique, 2008.

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 Editora, Coimbra, 2011.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2018.

Nunes, Duarte Rodrigues – Revistas e buscas no Código de Processo Penal, Gestlegal, Coimbra, 2019.

Nunes, Duarte Rodrigues – O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada, Gestlegal, Coimbra, 2019.

Ortiz Pradillo, Juan Carlos – "El registro «*online*» de equipos informáticos como medida de investigación contra el terrorismo (*online-Durchsuchung*)", *in* Terrorismo y Estado de Derecho, pp. 457 e ss., Iustel, Madrid, 2010.

Ramalho, David Silva – "A investigação criminal na *Dark Web*", *in* Revista de Concorrência e Regulação, Ano IV, n.ºs 14-15, pp. 383 e ss., Almedina, Coimbra, 2013.

Ramalho, David Silva – "O uso de *malware* como meio de obtenção de prova em processo penal", *in* Revista de Concorrência e Regulação, Ano IV, n.º 16, pp. 195 e ss., Almedina, Coimbra, 2013.

Ramalho, David Silva – "The use of malware as a mean of obtaining evidence in Portuguese criminal proceedings", *in* Digital Evidence and Electronic Signature Law Review, 11 (2014), pp. 55 e ss., *in https://journals.sas.ac.uk/deeslr/article/view/2125* (consultado em 10/07/2020).

Ramalho, David Silva – Métodos Ocultos de Investigação Criminal em Ambiente Digital, Almedina, Coimbra, 2017.

Ramos, Armando Dias – "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 49 e ss., Almedina, Coimbra, 2016.

Rodrigues, Benjamim Silva – Da Prova Penal, Tomo II, Bruscamente…A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 1.ª Edição, Rei dos Livros, Lisboa, 2010.

Roggan, Fredrik – "Präventive Online-Durchsuchungen", *in* Online-Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, pp. 97 e ss, Berliner Wissenschafts-Verlag, Berlim, 2008.

Roxin, Claus/Schünemann, Bernd – Strafverfahrensrecht, 27.ª Edição, C.H.Beck, Munique, 2012.

Singelnstein, Tobias – "Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche

Datenverarbeitung&Co", *in* Neue Zeitschrift für Strafrecht, 2012, pp. 593 e ss., C. H. Beck'sche Verlagsbuchhandlung, Munique e Frankfurt, 2012.

Tonini, Paolo – Manuale di Procedura Penale, 12.ª Edição, Giuffrè Editore, Milão, 2011.

Venâncio, Pedro Dias – Lei do Cibercrime, Anotada e Comentada, Coimbra Editora, Coimbra, 2011.

JURISPRUDÊNCIA

Tribunal Europeu dos Direitos Humanos

Acórdão Malone c. Reino Unido (de 2 de agosto de 1984), *in https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]}* (consultado em 09/07/2020).

Alemanha

Bundesverfassungsgericht

Sentença de 15 de dezembro de 1983 (1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83 e BvR 484/83), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html* (consultada em 09/07/2020).

Sentença do *Bundesverfassungsgericht* de 3 de março de 2004 (1 BvR 2378/98 e 1 BvR 1084/99), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/03/rs20040303_1bvr237898.html* (consultada em 09/07/2020).

Sentença de 27 de fevereiro de 2008 (1 BvR 370/07 e 1 BvR 595/07), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html* (consultada em 09/07/2020).

Sentença de 20 de abril de 2016 (1 BvR 966/09 e 1 BvR 1140/09), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html* (consultada em 09/07/2020).

Sentença de 6 de julho de 2016 (2 BvR 1454/13), *in https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/07/rk20160706_2bvr145413.html* (consultada em 09/07/2020).

Bundesgerichtshof

Sentença de 21 de fevereiro de 2006 [3 BGs 31/06, 3 BJs 32/05 - 4 - (12) - 3 BGs 31/06)], *in www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php* (consultada em 09/07/2020).

Sentença de 31 de janeiro de 2007 (StB 18/06), *in www.hrr-strafrecht.de/hrr/3/06/stb-18-06.php* (consultada em 09/07/2020).

Espanha

Tribunal Constitucional de España

Sentença n.º 49/1999, *in https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/3791* (consultada em 09/07/2020).

Estados Unidos

Supreme Court of the United States

Sentença Olmstead v. United States, 277 U.S. 438 (1928), *in* https://supreme.justia.com/cases/federal/us/277/438/ (consultado em 15/07/2020).

Sentença Goldman v. United States, 316 U.S. 129 (1942), *in* https://supreme.justia.com/cases/federal/us/316/129/ (consultado em 15/07/2020).

Sentença Silverman v. United States, 365 U.S. 505 (1961), *in* https://supreme.justia.com/cases/federal/us/365/505/ (consultado em 15/07/2020).

Sentença Berger v. New York, 388 U.S. 41 (1967), *in https://supreme.justia.com/cases/federal/us/388/41/* (consultado em 15/07/2020).

Sentença Katz v. United States, 389 U.S. 347 (1967), *in https://supreme.justia.com/cases/federal/us/389/347/* (consultado em 14/07/2020).

Sentença Chimel v. California, 395 U.S. 752 (1969), *in https://supreme.justia.com/cases/federal/us/395/752/* (consultado em 14/07/2020).

Sentença Coolidge v. New Hampshire, 403 U.S. 443 (1971), *in https://supreme.justia.com/cases/federal/us/403/443/* (consultado em 14/07/2020).

Sentença Couch v. United States, 409 U.S. 322 (1973), *in https://supreme.justia.com/cases/federal/us/409/322/* (consultado em 14/07/2020).

Sentença United States v. Miller, 425 U.S. 435 (1976), *in https://supreme.justia.com/cases/federal/us/425/435/* (consultado em 14/07/2020).

Sentença Andresen *v.* Maryland, 427 U.S. 463 (1976), *in https://supreme.justia.com/cases/federal/us/427/463/* (consultado em 14/07/2020).

Sentença Zurcher v. Stanford Daily, 436 U.S. 547 (1978), *in https://supreme.justia.com/cases/federal/us/436/547/* (consultado em 14/07/2020).

Sentença Rakas v. Illinois, 439 U.S. 128 (1978), *in https://supreme.justia.com/cases/federal/us/439/128/* (consultado em 14/07/2020).

Sentença Smith v. Maryland, 442 U.S. 735 (1979), *in https://supreme.justia.com/cases/federal/us/442/735/* (consultado em 14/07/2020).

Sentença Walter v. United States, 447 U.S. 649 (1980), *in https://supreme.justia.com/cases/federal/us/447/649/* (consultado em 14/07/2020).

Sentença United States v. Jacobsen, 466 U.S. 109 (1984), *in https://supreme.justia.com/cases/federal/us/466/109/* (consultado em 14/07/2020).

Sentença Riley v. California, 134 S. Ct. 2472 (2014), *in https://www.law.cornell.edu/supremecourt/text/13-132* (consultado em 16/07/2020).

United States Court of Appeals

Sentença National City Trading Corp. v. United States, 635 F.2d 1020 (2nd Circuit 1980), *in https://casetext.com/case/national-city-trading-corp-v-united-states-2* (consultado em 14/07/2020).

Sentença De Massa v. Nunez, 770 F.2d 1505 (9th Circuit, 1984), *in https://casetext.com/case/demassa-v-nunez* (consultado em 14/07/2020).

Sentença Klitzman, Klitzman and Gallagher v. Krut, 744 F.2d 955 (3rd Circuit, 1984), *in https://law.justia.com/cases/federal/district-courts/FSupp/591/258/23 88284/* (consultado em 14/07/2020).

Sentença United States *v.* Biasucci, 786 F.2d 504 (2nd Circuit, 1986), *in https://casetext.com/case/united-states-v-biasucci* (consultado em 14/07/2020).

Sentença United States *v.* Cuevas-Sanchez, 821 F.2d 248 (5th Circuit, 1987), *in https://casetext.com/case/us-v-cuevas-sanchez* (consultado em 14/07/2020).

Sentença United States v. Lin Lyn Trading, Ltd., 149 F.3d 1112 (10th Circuit, 1998), *in https://casetext.com/case/us-v-lin-lyn-trading-ltd-3* (consultado em 14/07/2020).

Sentença United States *v.* Hall, 165 F.3d 1095 (7th Circuit, 1998), *in https://casetext.com/case/us-v-hall-253* (consultado em 14/07/2020).

Sentença United States v. Carey, 172 F. 3d 1268 (10th Circuit, 1999), *in https://caselaw.findlaw.com/us-10th-circuit/1317424.html* (consultado em 15/07/2020).

Sentença Leventhal v. Knapek, 266 F3d 64 (2nd Circuit, 2001), *in https://caselaw.findlaw.com/us-2nd-circuit/1332549.html* (consultado em 15/07/2020).

Sentença Ferguson v. Charleston, 532 U.S. 67 (4th Circuit, 2001), *in https://supreme.justia.com/cases/federal/us/532/67/* (consultado em 14/07/2020).

Sentença Guest v. Leis, 255 F.3d 325 (6th Circuit, 2001), *in https://caselaw.findlaw.com/us-6th-circuit/1016277.html* (consultado em 14/07/2020).

Sentença United States *v.* Lifshitz, 369 F.3d 173 (2nd Circuit, 2004), *in https://openjurist.org/369/f3d/173/united-states-v-lifshitz* (consultado em 14/07/2020).

Sentença United States v. Heckenkamp, 482 F.3d 1142 (9th Circuit, 2007), *in https://www.casemine.com/judgement/us/5914b43eadd7b0493476b3d9* (consultado em 15/07/2020).

Sentença United States v. Forrester, 512 F.3d 500 (9th Circuit, 2007), *in https://caselaw.findlaw.com/us-9th-circuit/1452307.html* (consultado em 14/07/2020).

Sentença United States v. Ganoe, 538 F.3d 1117 (9th Circuit, 2008), *in https://caselaw.findlaw.com/us-9th-circuit/1169300.html* (consultado em 16/07/2020).

Sentença United States *v.* Perrine, 518 F.3d 1196 (10th Circuit, 2008), *in https://caselaw.findlaw.com/us-10th-circuit/1308994.html* (consultado em 14/07/2020).

United States District Court for the District of Connecticut

Sentença United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001) (2001), *in https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/* (consultado em 15/07/2020).

United States District Court for the Southern District of New York

Sentença United States v. Wey, 52 F. Supp. 3d 237 (S.D.N.Y. 2017) (2017), *in https://casetext.com/case/united-states-v-wey-3* (consultado em 15/07/2020).

United States District Court for the North District of Ohio, Western Division

Sentença United States *v.* Skeddle, 989 F. Supp. 890 (N.D. Ohio 1997), *in https://law.justia.com/cases/federal/district-courts/FSupp/989/890/1528661/* (consultado em 14/07/2020).

United States District Court for the Southern District of Texas

Sentença In re Warrant to Search Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (2013), *in https://casetext.com/case/in-re-search* (consultado em 14/07/2020).

United States District Court for the District of Vermont

Sentença United States v. Hunter, 13 F. Supp. 2d 574 (1998), *in https://law.justia.com/cases/federal/district-courts/FSupp2/13/574/2311683/* (consultado em 14/07/2020).

United States District Court for the Western District of Washington

Sentença United States v. Gorshkov, 2001 WL 1024026, U.S. Dist. LEXIS 26306 (2001), *in https://itlaw.wikia.org/wiki/U.S._v._Gorshkov* (consultado em 15/07/2020).

Supreme Court of Minnesota

Sentença O' Connor v. Johnson, 287 N.W.2d 400 (Minn. 1979), *in https://www.casemine.com/judgement/us/5914930cadd7b049345a31c4* (consultado em 14/07/2020).

Massachussets Superior Court

Sentença Commonwealth *v.* Cormier, No. 09-1365, 2011, WL 3450643 (2011)¸ *in https://www.casemine.com/judgement/us/59146083add7b0493422ed7e* (consultado em 14/07/2020).

Court of Appeals of Wisconsin

Sentença State *v.* Schroeder, 2000 WI App 128, 613 N.W.2d 911, 237 Wis. 2d 575 (2000), *in https://www.courtlistener.com/opinion/2221561/state-v-schroeder/* (consultado em 15/07/2020).

Itália

Suprema Corte di Cassazione

Jurisprudência fixada

Sentença das *Sezioni Unite* de 28 de abril de 2016 – 1 de julho de 2016, n.º 26889, *in www.archiviopenale.it/intercettazioni--cass-sez-un-1-luglio-2016-(cc-28-aprile-2016)-scurato/contenuti/6142* (consultada em 07/07/2016).

Outra Jurisprudência

Sentença de 30 de maio de 2017-20 de outubro de 2017 (*Sezione* V, n.º 48370), *in www.archiviopenale.it/intercettazioni--cass-sez-v-20-ottobre-2017-(cc-30-maggio-2017)-occhionero-ed-altri/contenuti/6703* (consultada em 07/07/2016).

Sentença de 8 de março de 2018 – 9 de outubro de 2018 (*Sezione* VI, n.º 45486), *in www.archiviopenale.it* (consultada em 07/07/2016).

Sentença de 25 de junho de 2019 – 17 de dezembro de 2019 (*Sezione* I, n.º 50972), *in www.salvisjuribus.it* (consultada em 07/07/2016).