
# OS DIREITOS FUNDAMENTAIS X SEGURANÇA PÚBLICA: A ADMISSIBILIDADE DE MÉTODOS OCULTOS DE INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL

**THIAGO HARTMANN MARTINEZ – Nº 27019**

**Mestrado Científico em Ciências Jurídico-Criminais (2.º Ciclo)**

**Regente: Professor Doutor Paulo de Sousa Mendes**

**Ano letivo: 2019**

## AGRADECIMENTOS

Dedico este trabalho aos meus pais, Diego e Nadja, sem os quais nada seria possível.

**Resumo:**

Inspirado na evoluçao tecnológica dos últimos anos e nas transformações que a mesma vem causando no Direito Processual Penal e na criminalidade que atinge a sociedade nessa nova Era Digital em que vivemos, o presente trabalho tem a pretensão de estudar os metódos ocultos de investigação criminal em ambiente digital, tendo em vista que os sistemas infomáticos se transformaram em uma rica fonte de provas das mais variadas formas de criminalidade, inclusive da mais grave, como o terrorismo e o crime organizado. Assim, levando em conta as pecurialidades e dificuldades na obtenção da prova digital, o Estado, no dever de acompanhar a evolução tecnológica e equiparar as armas para o combate dessa criminalidade em ambiente digital e da criminalidade mais grave, passou a contar com o uso de *malware* (como os cavalos de Tróia) e do agente encoberto para obtenção da prova contida em ambiente digital. Contudo, da análise das duas figuras, constatou-se que a primeira ainda não tem previsão legal expressa no ordenamento jurídico Português (ainda que já tenha em diversos outros países); enquanto que a segunda já o tem. Ainda, tendo em vista a elevada restrição que esses e outros métodos ocultos de investigação criminal são para os direitos fundamentais dos investigados (como para a privacidade/intimidade, inviolabilidade do domicílio, direito a não autoincriminação, confidencialidade e integridade dos sistemas informáticos, entre outros), concluiu-se pela necessidade de criação de um sistema único e geral dos métodos ocultos no ordenamento jurídico Português (já que são previstos em diplomas extravagantes sem qualquer unidade), onde devem ser estabelecidos os princípios e regras que o aplicador do direito deve seguir para utilizar os mesmos de maneira proporcional no caso concreto, visando alcançar o equilíbrio entre direitos fundamentais e segurança pública.

**Palavras-chave:**

Agente encoberto**;** direitos fundamentais**;** investigação criminal em ambiente digital**;** *malware*; metódos ocultos**.**

***Abstract:***

*Inspired by technological evolution in the last years, as well as in the transformations which have happened in Penal Process Law and criminality, this study aims at hidden methods of criminal investigation in the digital environment, bearing in mind the fact IT systems have turned into a rich source of evidence for all sort of crimes, including the most harmful ones, such as terrorism and organized crime. Therefore, taking into account the specificities and dificultes in obtaining digital evidence, the State, havin as duty the follow-up on technological advances, must catch up with the weapons to combat such criminality, doing such by making use of malware and undercover agents. Nevertheless, by the analysis of such of both tools, this study reaches the conclusion the former does not have express legal grounds in the Portuguese law, despite the fact it does elsewhere; while the latter already does. Moreover, due to the high restriction that these methods cause to the suspects' fundamental rights (such as privacy, domicile inviolability, non-discrimination, confidenciality and IT systems integrity), the study also reaches the conclusion that there is a need to draft a specific and general regime in Portuguese law for such hidden methods, in which there must be principles and rules to guide the law operators on a case-by-case basis. That way both fundamental rights and public security can be achieved.*

***Keywords:***

*Criminal investigation in digital environment*; *fundamental rights*; h*idden methods; malware; undercover agent*.

**ÍNDICE**

# INTRODUÇÃO

São inegáveis as grandes e aceleradas transformações técnico-científicas das últimas décadas, trazendo consigo mudanças em todos os níveis da organização da vida individual ou comunitária, e em todas as formas da experiência, ao nível do ser ou da relação. Contudo, nessas mesmas últimas décadas a criminalidade também sofreu grandes mudanças e avanços, onde a evolução do crime organizado e violento e a ameaça do terrorismo se uniram com a disseminação de novas tecnologias capazes de fomentar a prática de ilícitos e a reduzir a possibilidade de detecção dos mesmos, capacitando aos criminosos permanecerem na sombra do anonimato e da impunidade.

Em razão disso, aumentou-se a sensação de insegurança, gerada pelos novos riscos da pós-modernidade e agravada pelo sucesso de ataques terroristas em grandes capitais do mundo, levando a sociedade a tolerar a imposição de medidas progressivamente mais restritivas de direitos fundamentais, como a privacidade e liberdade, sob o pretexto da recuperação da segurança por parte do Estado.

Dessa forma, o Estado e o Direito, mais precisamente o Direito Processual Penal, se viram no dever de adaptar-se à essa evolução tecnológica e criminal e a equipar-se com um novo arsenal de métodos de investigação e obtenção de prova capazes de combater essa onda de criminalidade que assola a sociedade. Pois se de um lado a evolução tecnológica facilita a prática de ilícitos das mais variadas formas, mostrando-se um verdadeiro atrativo para os criminosos, do outro lado ela alarga as possibilidades de investigação criminal, aumentando as probabilidades de sucesso do Estado na perseguição de criminosos.

Nesse contexto, se inserem a investigação criminal em ambiente eletrônico-digital e as provas digitais daí decorrentes. Hoje, esse tipo de prova é imprescindível para o processo penal. Não só para a nova criminalidade informático-digital, como também para a criminalidade clássica, onde o investigador pode, por exemplo, se deparar com um criminoso que utilizou o seu computador para cometer vários crimes, ou em uma investigação de homicídio poderão ser encontradas informações importantes em um computador portátil onde constam vários e-mails referentes ao crime ou um plano para arquitetar o rapto de uma pessoa. Ou ainda, uma organização criminosa ou um grupo terrorista pode armazenar todo o seu sistema hierárquico e seu funcionamento em um sistema informático.

Independentemente do caso, pode-se afirmar que a informação probatória imprescindível se encontra armazenada ou contida em sistemas ou redes informáticas ou em repositórios eletrônicos-digitais de armazenamento, e para capturar e condenar os suspeitos, é necessário aceder e recolher a prova digital que se encontra em tais equipamentos eletrônicos-digitais, prova essa que vem sustentando cada vez mais os mais diversos tipos de despachos de acusação.[1]

Mas devido à complexidade criminalística imposta pelo avanço tecnológico, resultando nas peculiaridades e dificuldade na obtenção da prova armazenada em computadores, o Estado, na obrigação de salvaguardar a segurança dos seus cidadãos, se viu na necessidade de utilizar não apenas novos métodos de investigação, mas, sobretudo novos *métodos ocultos* de investigação para obtenção da prova contida em sistemas informáticos. Por métodos ocultos de investigação entende-se como toda intromissão por parte dos órgãos de investigação nos processos de ação, interação, informação e comunicação das pessoas investigadas, sem que as mesmas tenham conhecimento disso, de modo que o secretismo da medida é fundamental para o sucesso das investigações.[2] Em ambiente digital, os métodos ocultos utilizados com maior frequência (e que serão os abordados aqui) são o agente encoberto e a utilização de *malware* para obtenção de prova (*buscas online*).

Em muitos casos a obtenção de prova em ambiente digital por métodos *abertos*, como por exemplo o exame forense do disco rígido e dos elementos periféricos de equipamentos informáticos (assim como de qualquer outro dispositivo eletrônico de comunicação e armazenamento) por meio de uma busca e apreensão, se mostra inadequada e até mesmo impossível para obtenção de provas (assumindo que não se tenha acesso físico ao sistema informático, o que é comum em investigações em ambiente digital). Assim, se faz cada vez mais necessário o uso de sofisticados instrumentos eletrônicos e programas informáticos capazes de conseguir a interceptação e gravação em tempo real, de forma oculta e a distância de toda informação contida e transmitida pelo equipamento informático visado, aproximando-se tais atuações policiais do denominado *hacking* ou intrusão informática, onde é possível também

[1] RODRIGUES, Benjamim Silva, Das escutas telefônicas à obtenção da prova em ambiente digital. 2ª Edição revisada, atualizada e aumentada, Coimbra: Editora Coimbra, 2009, p. 567.
[2] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia ter sido diferente,* Coimbra: Coimbra Editora, 2009, p. 105.

contornar as diversas técnicas antiforenses existentes (que serão tratadas posteriormente).[3]

Contudo, a utilização de tais métodos ocultos revela um alto nível de lesividade de direitos e garantias fundamentais, como a privacidade/intimidade, palavra, imagem, inviolabilidade do domicílio, sigilo das telecomunicações, confidencialidade e integridade dos sistemas técnico-informacionais, bem como o princípio *nemo tenetur se ipsum accusare* e o direito ao silêncio, entre outros. Nesse contexto, estamos diante de um conflito onde de um lado está o interesse público da realização da justiça e sucesso das investigações criminais (tendo em vista a eficácia dos métodos ocultos para tanto), e do outro o interesse público da tutela dos referidos direitos fundamentais. De um lado da balança está a segurança pública, e do outro a privacidade e liberdade.[4]

É nesse sentido que o presente trabalho, baseando-se na obra de David Silva Ramalho (*Métodos ocultos de Investigação Criminal em Ambiente Digital*, 2017), busca analisar a utilização de métodos ocultos de obtenção de prova em ambiente digital e os direitos fundamentais mais atingidos com isso, de modo a encontrar uma possível solução para tal conflito e para admissibilidade das provas obtidas com tais medidas, tendo em vista que o legislador português não prevê a matéria dos métodos ocultos de maneira satisfatória, já que não há um sistema geral que rege os mesmos. Eles são previstos em diplomas extravagantes, sem qualquer unidade, e se estamos falando de medidas de investigação limitativas de direitos fundamentais, não podemos contentar-se com insuficiências legislativas ou analogias.

Para isso, primeiro serão analisadas as peculiaridades e características da prova digital e da sua obtenção, demonstrando também os diferentes mecanismos existentes para dificultar o rastreamento da mesma e do seu respectivo autor, bem como da sua recolha (as chamadas medidas antiforenses). Após, serão abordados os métodos ocultos de uma maneira geral, sob a perspectiva da busca pela verdade no processo penal.

Em seguida, trataremos dos progressos técnico-científicos que deram lugar a novos e variados métodos ocultos de investigação, mas que consequentemente atingiram uma variedade de direitos fundamentais, analisando os mais atingidos separadamente e a solução que a doutrina e jurisprudência mais avançada sobre a matéria têm dado para essa questão.

---

[3] PRADILLO, Juan Carlos Ortiz. *Hacking'legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquencia informática*, Revista Aranzadi de Derecho y Processo Penal, n° 26, 2011-2, Navarra: Thomson Reuters Aranzadi , p. 75-76.
[4] ANDRADE, Manuel da Costa. 2009, p. 105-106.

Por fim, serão expostos e estudados os métodos ocultos mais frequentes e eficazes em ambiente digital, e na sequencia será buscada uma solução com base em princípios e regras que o legislador e aplicador do direito devem seguir para que os métodos ocultos de obtenção de prova em ambiente digital possam ser utilizados de uma maneira legítima e admissível no processo penal de um Estado Democrático de Direito, visando a menor lesividade possível dos direitos fundamentais do visado, respeitando sempre as exigências do princípio da proporcionalidade.

# I. O CASO UNITED STATES VS. ROSS ULBRICHT

Na obra Métodos Ocultos de Investigação Criminal em Ambiente Digital, Ramalho traz o caso conhecido como *United States Vs Ross Ulbricht*[5], onde o autor relata o famoso mercado digital online de drogas conhecido como *The Silk Road*, localizado na *Deep Web*[6] e criado em 2011, onde os seus utilizadores dispunham de um variado arsenal de produtos, desde cocaína e LSD, entre outros. O que tornou este *website* famoso e de grande procura foi o fato de ter aliado duas tecnologias de anonimato que tornavam teoricamente impossível de detectar a localização dos servidores e dos seus utilizadores, bem como permitiam que as transações efetuadas pelos usuários não fossem descobertas por terceiros.[7]

Uma dessas tecnologias de anonimato é o *TOR (The Onion Router)*, um programa informático que torna a navegação na internet anônima, é uma navegação em certas partes da Internet inacessíveis através dos comuns *browsers*, escondendo o IP dos utilizadores e dos servidores que se encontram os *websites.* A segunda tecnologia é a *Bitcoin*, uma moeda virtual que permite esconder a identidade do seu proprietário perante o outro participante da transação, e, principalmente, perante quaisquer entidades externas, como instituições financeiras ou o próprio Estado. A combinação desses dois ingredientes foi essencial para que o *Silk Road* funcionasse abertamente, permanecendo indetectável perante o olhar das autoridades. Além disso, não havia interação alguma entre comprador e vendedor nas transações realizadas pelo *website*, onde o comprador apenas efetuava um registro com nome de utilizador e senha e selecionava no catálogo qual produto desejava, fazendo o pagamento em *bitcoins* para o *Silk Road*, e dias mais tarde receberia a encomenda. Já o vendedor, receberia sua quantia no momento em que os administradores do *website* tivessem notícia do envio da mercadoria, retendo para eles uma comissão. Mas ainda que a interação não fosse necessária, as partes poderiam conversar através de mensagens privadas por um *chat* que o *website* oferecia, além de

[5] As informações e peças processuais sobre esse caso estão disponíveis no site: http://freeross.org/category/documents/; e as infomações do caso aqui escritas foram retiradas do livro: RAMALHO, David Silva. *Métodos ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017, p 27-33.

[6] A *Deep Web* é uma área da Internet não acessível ao utilizador comum, não surgindo nos vulgares motores de busca, sendo o seu acesso efetuado através da denominada *Freenet* (*software* que permite o total anonimato nessa área invisível da Internet) ou através do TOR (*The Onion Router)*. O principal objetivo da *Deep Web* e dos referidos *softwares* é manter o anonimato dos seus utilizadores, tornando suas atividades e localizações indetectáveis ás forças policiais.

[7] RAMALHO, David Silva, 2017, p 27.

oferecer um fórum para os utilizadores trocarem conselhos para evitar a detecção ou como utilizar técnicas de criptografia e medidas de segurança informática.[8]

Assim, em razão da dificuldade técnica em detectar a localização dos servidores do *Silk Road* e dos seus utilizadores, agentes de várias autoridades policias norte-americanas passaram a desenvolver ações encobertas no *website.* Carl Force IV era um desses agentes, que se fez passar por um traficante de drogas chamado *Nob*, e que, por meio de comunicações privadas, conseguiu ganhar a confiança de DPR (*Dread Pirate Robert)*. Tal confiança foi conquistada com base em informações privilegiadas de que dispunha, informando DPR de detalhes de outras investigações policias focadas em outros membros do *Silk Road* e de buscas iminentes, afirmando ter um informante na policia. Carl Force também conquistou a confiança de outros membros da administração do *Silk Road*, permitindo-lhe simular uma venda de cocaína com um colaborador em particular, e após obter o seu endereço, participar da detenção do mesmo. No momento em que foi publicada a noticia da detenção do vendedor, DPR pediu para que *Nob* matasse o mesmo, o que foi simulado pelo FBI.[9]

Após várias tentativas frustradas de acesso ao IP do servidor do qual se encontrava armazenado o *Silk Road*, no dia 5 de junho de 2013 o FBI conseguiu obtê-lo e localizar sua origem na Islândia, graças ao que foi dito como uma falha na configuração do sistema. De imediato, foi requerida a cooperação das autoridades islandesas para que extraíssem um copia integral do servidor. Contudo, importante referir que o modo como o FBI obteve o IP tem sido considerado, pela defesa como por alguns peritos informáticos, inconsistente, improvável e contraditório com a documentação juntada aos autos, existindo suspeitas de que o acesso ao servidor tenha ocorrido com recurso a tecnologias de *hacking* (o que será abordado a frente). E ao ser requerida pela defesa para demonstrar os registros da atividade forense que levou à identificação do IP, a acusação respondeu que tais elementos probatórios não foram guardados.[10]

A investigação do *Silk Road* foi complementada por buscas de informação na internet aberta, bem como por informações obtidas na *Dark Web* e nos registros da HSI (*Homeland Security Investigations).* Com base em uma busca por referências ao *Silk Road* no motor de busca *Google,* foram encontradas algumas mensagens datadas de

[8] *Idem*, p. 27-28.
[9] *Idem*, p. 29.
[10] *Idem*, p. 30.

janeiro e fevereiro de 2011, quando o *Silk Road* ainda estava na sua fase inicial. As mensagens foram publicadas em diversos fóruns por um usuário chamado *altoid*, que parecia estar querendo publicitar o então novo mercado digital, e em outras situações o usuário procurava um especialista em informática da comunidade *Bitcoin*, solicitando que qualquer informação fosse enviada para o e-mail rossulbricht@gmail.com.[11]

Posteriormente, em 2013, foi interceptada uma encomenda vinda do Canadá para a residência de Ross Ulbricht, contendo documentos falsos de identificação com sua fotografia, sendo que quando questionado por agentes da HSI, Ross mencionou que qualquer pessoa poderia ter feito aquela encomenda para o seu endereço pelo site chamado *Silk Road.* Como se não bastasse, após uma pesquisa em fontes abertas pelo nome de Ross Ulbricht, foi possível descobrir que esse partilhava com DPR não apenas o mesmo fuso horário, como também os mesmos interesses pessoais, principalmente em política e economia. Assim, a união de todos esses elementos deu início a uma vigilância física de Ulbricht, buscando o cruzamento da sua atividade no mundo *online* com sua atividade no mundo físico. Os resultados demonstraram que o acesso de Ross Ulbricht à internet estava sincronizado com a entrada *online* de DPR no *website Silk Road.*[12]

Então, no dia 1 de outubro de 2013, Ross foi á biblioteca Glen Park em San Francisco, ligou o seu computador e conectou-se ao *Silk Road.* Usando o usuário de nome *Dread Pirate Robert* (DPR), passou a trocar mensagens *online* com *Cirrus* (usuário que supunha conhecer, mas que no momento era controlado por um agente da HSI), quando então agentes do FBI passaram a simular uma discussão na biblioteca. No instante em que Ross se virou para ver o que acontecia, o computador foi retirado da sua frente e apreendido. Tal atitude se fez necessária pelo fato de o próprio DPR ter referido no *Silk Road* que o seu computador portátil estava equipado com medidas antiforenses que, em caso de suspeitas da presença de agentes policiais, tornariam instantaneamente o conteúdo do computador inacessível. A partir disso, no computador foi encontrada vasta prova do envolvimento de Ross na criação do *Silk Road*, além de um diário pessoal onde introduzia tanto fatos sobre a sua vida intima como dados da gestão do *website.*[13]

[11] *Idem*, p. 30-31.
[12] *Idem*, p. 31.
[13] *Ibidem.*

No dia 30 de maio de 2015 Ross Ulbricht foi condenado a prisão perpétua sem possibilidade de liberdade condicional cominada com a obrigação de restituição de $183.961.921,00 pela prática dos crimes de auxilio á distribuição de drogas na Internet, continuação de uma organização criminosa, comparticipação na prática de crimes de acesso ilegítimo, fraude com recurso a documentos de identificação e comparticipação em lavagem de dinheiro. Também foi publicada, no dia 25 de março de 2015, queixa criminal contra o agente da DEA Carl Force IV e o agente dos Serviços Secretos Shaun Bridges, por suspeita da prática de crimes de suborno, extorsão, fraude, conflitos de interesse e abuso de confiança, alegadamente praticados no âmbito da investigação do caso *Silk Road.* Tido como o principal agente encoberto na investigação, Carl Force IV teria, entre outras atividades ilícitas, criado outras identidades fictícias não autorizadas através das quais teria se comunicado com DPR e o extorquido em troca da promessa de não revelação de dados às autoridades, ou da venda de informações da investigação por cerca de $100.000,00, os quais foram realmente pagos. Já Shaun Bridges, teria, entre outras condutas, aproveitado o acesso privilegiado ao *Silk Road* para se apropriar de quantias que ultrapassam os $250.000,00 em *bitcoins.*[14]

Atualmente, o caso do *Silk Road* se encontra na fase recursal, mas independentemente do resultado da decisão de segunda instância, é inegável, como destaca Ramalho, que o caso apresenta importantes e delicadas questões sobre prova digital e privacidade, demonstrando as dificuldades trazidas à investigação pelas mais frequentes técnicas antiforenses, tornando os métodos tradicionais de obtenção de prova insuficientes face às novas realidades do cibercrime, sendo necessário recorrer aos novos métodos ocultos de investigação criminal em ambiente digital. Para o autor, a questão acaba por trazer também a problemática do acesso a diário e informações pessoais em formato digital e a necessidade de aplicação de requisitos estritos de controle da atividade de recolha de prova em todas as fases da investigação, com vista a garantir tanto a cadeia de custódia no plano forense, bem como garantir que a prova seja obtida em cumprimento às exigências constitucionais que permitem sustentar sua validade.[15]

## 1. A prova digital e as peculiaridades da sua obtenção

[14] *Idem*, p. 31-33.
[15] *Idem*, p. 33.

Nunca como hoje todas as pessoas do mundo estão tão perto, à distância de um "clique", e nunca como hoje a informação circulou de uma maneira tão livre e rápida. Mas acompanhando a evolução tecnológica, o comportamento criminoso também evoluiu. Atualmente, praticamente todos tem acesso a um computador, e isso pode representar um risco para a sociedade, tendo em vista que se os computadores facilitam tudo em nossas vidas, também facilitam a prática de crimes.

O atrativo para o "criminoso digital" é grande, já que corre poucos riscos e acredita que jamais será descoberto, permanecendo nas sombras do anonimato proporcionado pela rede, tornando a investigação e detecção deste tipo de crime e a obtenção das provas armazenadas no seu computador algo muito difícil ou até mesmo impossível.

Esses criminosos estão cada vez mais criativos e inteligentes, sendo possível encontrar todo o tipo de ilícito na Internet, como fraudes, ameaças, pornografia infantil, violação de direitos de autor, devassa da vida privada, falsidade informática, dano e sabotagem informática, entre inúmeros outros tipos de crimes, podendo até mesmo por em causa a segurança dos próprios países (como com o ciberterrorismo), sem falar nos crimes que acontecem no mundo material e deixam seus rastros como prova no mundo digital, tendo em vista a utilização de computadores e dispositivos móveis para quase tudo, até mesmo para arquitetar um homicídio ou um ataque terrorista, por exemplo. Nesse contexto, se inserem a investigação criminal em ambiente eletrônico-digital e as provas digitais daí decorrentes. Conforme apontado por Rodrigues, a prova digital encontra-se presente em diversas plataformas do nosso dia a dia, em computadores, *tablets, smartphones,* dispositivos USB, câmaras digitais, gravadoras de áudio, sistemas de vídeo vigilância, em movimento por redes de comunicações eletrônicas, entre outros locais. Cada uma destas fontes de prova digital pode conter várias categorias de provas, e por sua especificidade, pode impor diferentes meios de recolha, que, naturalmente, não podem ser comparados com os meios de recolha de prova física.[16]

Assim, pode-se dizer que o aumento da utilização de tais ferramentas na sociedade moderna levou ao aumento da relevância da prova digital no combate da criminalidade, tendo em vista que tal prova vem sustentando cada vez mais os mais diversos tipos de despachos de acusação, dando até mesmo origem a uma nova forma de investigação, a Ciência Forense Digital ou *digital/computer forensic*. Ela pretende

[16] RODRIGUES, Benjamim Silva, 2009, p. 534-536.

orientar a investigação criminal em ambiente digital, sendo considerada como uma resposta ás exigências que se fizeram sentir, ao nível da lei processual penal, para a perseguição da criminalidade informático-digital.[17]

Segundo JOHN R. VACCA[18], *digital forensic* trata-se da análise forense dos computadores, a descoberta eletrônica, a descoberta de prova eletrônica, a descoberta e recuperação de dados, traduzindo-se na análise dos componentes do computador para efeitos probatórios. Ou seja, é a recolha, preservação, análise, e apresentação da prova eletrônico-digital. E de fato, para efeitos probatórios, acessar ao local do crime eletrônico-digital exige o respeito de vários protocolos, sob pena desse tipo de prova não poder ser admitido em juízo, estando aí presente a necessidade de manutenção da "*chain of custody*" ou "cadeia de controle" da produção da prova forense digital.[19]

Nessa linha, pode-se definir a prova digital, nas palavras de Benjamim Silva Rodrigues, como

> "qualquer fluxo informacional ou comunicacional digital, que, estaticamente, se encontre armazenado, tratado ou processado, ou, pelo contrário, dinamicamente, seja transmitido, veiculado ou não por meio das redes informáticas ou de serviços e comunicações electrónicas, quer ao nível de um ciclo informacional e comunicacional fechado ou aberto, privado ou público."[20]

De uma maneira mais simples, o SWGDE (*Scientific Working Groupon Digital Evidence*) define a "*digital evidence"* como qualquer informação com valor probatório que se encontre armazenada ou é transmitida sob a forma binária[21]. Ou seja, é a prova que se apresenta na forma digital, e não em papel ou outro meio tangível.

Para melhor elucidar a diferença na obtenção da prova física e da prova digital, preciso é o exemplo de Orin S. Kerr[22], onde demonstra as evidentes diferenças entre a investigação criminal de um assalto a um banco e a investigação a um crime de acesso ilegítimo ao mesmo banco, com a subtração das mesmas quantias, mas em formato digital. No primeiro caso, serão inquiridas testemunhas, como funcionários e clientes do banco, que fornecerão informações relevantes como, por exemplo, o aspecto ou a voz

[17] *Idem*, p, 535.
[18] VACCA, John R., *Computer Forensics, Computer Crime Scene Investigation.* Charles River Media, Inc., Hingham, Massachusetts, 2002, p. 4.
[19] RODRIGUES, Benjamim Silva, 2009, p. 536.
[20] *Ibidem.*
[21] Informação disponibilizada no site https://www.swgde.org/. Acesso em 12/04/2017.
[22] KERR, Orin S., "*Digital evidence and the new Criminal Procedure",* Columbia Law Review, Vol. 105, n° 1 (Janeiro de 2005), p. 281-289.

do assaltante, serão recolhidas e analisadas impressões digitais e objetos eventualmente deixados na cena do crime, ou serão procurados carros semelhantes ao utilizado na fuga.

Já no segundo caso não há testemunhas ou prova física, nem sequer garantia de que o assaltante esteja no mesmo continente do assalto, mas há tão somente, como diz o autor, "zeros e uns de eletricidade". Sendo assim, caberá ao investigador, primeiramente, tentar obter o endereço IP de origem do "assaltante", todavia, isto apenas lhe permitirá saber a origem da comunicação a partir do último sistema informático de onde partiu a comunicação. E caso o assaltante tenha utilizado vários fornecedores de serviço como intermediários, é possível que seja necessário procurar junto dos mesmos os registros de origem da comunicação. Sendo otimista, ao encontrar o fornecedor de serviço inicial, será possível detectar a origem da comunicação e, talvez, o endereço da fatura do utilizador, o que permitirá fazer uma busca ao respectivo local e apreender o computador do qual partiu a comunicação eletrônica.[23]

E para a recolha da prova de relevância, que dificilmente será vista por um utilizador leigo, não será possível se socorrer dos mesmos investigadores do assalto físico ao banco, sendo necessário recorrer a um especialista em Ciência Forense Digital, que terá capacidade de utilizar procedimentos e ferramentas forenses apropriadas, como por exemplo, recuperar ficheiros eliminados, encontrar registros da conta utilizada, bem como reconstruir a atividade do assaltante. Mas para que essa prova não seja irremediavelmente contaminada, tornando-se inutilizável para o processo penal, é necessário que o investigador siga as regras forenses aplicáveis e os preceitos reguladores da recolha de prova em processo penal.[24]

Em suma, Kerr alerta para o fato de que o mundo virtual é diferente do mundo material, de modo que nem a semelhança conceitual das infrações, do bem jurídico afetado por elas, e nem a identidade terminológica em ambos os mundos, são capazes de ultrapassar essa diferença. E principalmente, o autor alerta que no plano processual, a prova digital não pode ser considerada como uma derivação da prova física, pois tratam-

[23] *Ibidem.* Esse mesmo exemplo é utilizado de uma maneira parecida por Benjamim Silva Rodrigues na obra referida anteriormente (2009, p. 568), quando o autor menciona o caso do assalto ao banco. O assalto pode ser realizado com o recurso de uma arma de fogo e deslocação ao local com ameaça à integridade física dos funcionários do banco se não entregarem o recheio do cofre (estando a prova presente aqui em ambiente físico). Ou o assalto pode ser realizado de forma mais sofisticada, onde o perito informático pode introduzir uma "rotina" no sistema ou rede informáticas do Banco e, a cada movimento, obter, de forma reiterada e automática, a transferência de dinheiro do Banco para uma conta, criada pelo mesmo cibercriminoso, num Banco situado num paraíso fiscal de Gilbraltar (estando a prova aí presente em ambiente digital).

[24] RAMALHO, David Silva, 2017, p. 103.

se de realidades distintas que deverão ser objeto de diferentes enquadramentos jurídicos, livres de amarras da analogia e da subsidiariedade de regimes planejados para a prova física. Em razão disso, a prova digital deve ser dotada de um regime autônomo, com mínimas e apenas necessárias remissões para normas aplicáveis ao mundo físico, tendo em vista o conjunto de especificidades pertencentes a prova e ao mundo digital, tornando imperioso a existência de normas que contemplem estas especificidades, incluindo garantias de fidedignidade na recolha e preservação da cadeia de custódia da prova recolhida.[25]

Portanto, se a obtenção dessa prova que se encontra em ambiente digital não pode ocorrer nos mesmos modos em que ocorre a prova física de qualquer outro crime, deve-se recorrer, na maioria dos casos, a referida Ciência Forense Digital. Assim, para melhor entendermos a árdua tarefa existente na obtenção da prova digital, se mostra pertinente referirmos certas características que a mesma possui, conforme ensina Benjamim Silva Rodrigues. Um dos aspectos mais importantes para os investigadores forenses digitais é ter presente que a prova eletrônico-digital é efêmera, possuindo um caráter temporário ou de não durabilidade, motivo pelo qual a sua colheita muitas vezes requer maior celeridade e cuidados. Do mesmo modo, a prova digital é frágil, susceptível de alterabilidade e instabilidade, de modo que ela não possui a estabilidade que reconhecemos aos documentos impressos, sendo que basta a retirada de um *"bit"* para alterar o documento informático, ou seja, a prova digital. Ainda, outras características que impõe dificuldades ao investigador forense resultam da aparente imaterialidade ou invisibilidade da prova digital, e da sua complexidade ou codificação, ao ponto que a identificação da mesma pressupõe o uso de determinadas técnicas e conhecimentos científicos que, ao não estarem presentes, não só não permitirão captar tal tipo de prova, como levarão à sua perda ou alteração, invalidando a sua força probatória em juízo. Outro fator importante é a dispersão da prova eletrônico-digital, tendo em vista que a mesma, em algumas situações, se espalha por terminais, computadores, e redes que se estendem por uma vasta área espacial ou geográfica, contrariando a criminalidade do mundo analógico, que ocorre em ambiente físico e concentrado.[26]

Sobre isso, devemos ter presente que para a obtenção da prova digital que se encontra no estrangeiro, a expressão "a Internet não conhece fronteiras" favorece ao

[25] *Idem*, p. 104.
[26] RODRIGUES, Benjamim Silva, 2009, p. 576-578.

delinquente, porque no plano policial as fronteiras nacionais se convertem em autênticos obstáculos para os legítimos fins da investigação e recolha de evidências do delito. Como afirma Pradillo, as forças e corpos de segurança devem respeitar a soberania de outros países e, como normal geral, não podem levar a cabo atividades de investigação e obtenção de provas fora da sua jurisdição.[27]

Para corroborar com essa problemática, devemos ter em conta que a deslocalização da informação armazenada é cada vez mais habitual com as técnicas de computação em nuvem (*Cloud Computing*), onde a informação se armazena de maneira permanente em servidores alojados em qualquer parte do mundo e através do acesso a Internet são enviados caches temporários ao computador ou *smartphone* do cliente.[28]

Em virtude de situações como essa é que os delitos cometidos através da Internet podem ser enquadrados como "delitos à distância": quando o resultado habitual entre o lugar em que o sujeito praticou o ato ilícito é diferente do lugar em que se produziu a ofensa ao bem jurídico, existindo uma notável distância geográfica que obriga determinar a competência territorial entre os órgãos jurisdicionais. Para contornar tais questões, a principal solução é aumentar a cooperação judicial internacional na luta contra essa nova ameaça global. Os denominados "registros transfronteiriços de equipamento informáticos" (*Cross-Border Searchs*) já se encontram expressamente previstos tanto em determinadas leis domésticas, como em certos tratados e textos internacionais.[29]

Em nível internacional, seu uso legal já havia sido proposto na Recomendação R (95) 13 do Conselho da Europa[30], de modo que as autoridades possam estender ao registro de equipamentos informáticos a outros sistemas que estejam conectados ao equipamento originariamente investigado e apropriar-se dos dados nele armazenados, inclusive quando tais sistemas se encontrarem em uma jurisdição estrangeira. A União Europeia também era partidária de admitir os registros transfronteiriços em determinados casos excepcionais ou de urgência, como por exemplo:

---

[27] PRADILLO, Juan Carlos Ortiz, *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, 2013, p. 12-13. Disponível em: http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf. Acesso em 10/04/2018.

[28] Sobre isso, ver: RAMALHO, David Silva. A recolha da prova em sistemas de computação em nuvem. In Revista de direito intelectual, Nº 2, Coimbra, 2014, p. 123-162.

[29] PRADILLO, Juan Carlos Ortiz. *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, 2013, p. 13.

[30] Recomendação R (95) 13, do Comité dos ministros do Conselho da Europa, de 11 de setembro de 1995, relativa aos problemas da legislação processual penal conectados ás tecnologias de informação.

> "*para impedir la destrucción o alteración de pruebas de un delito grave o para impedir la comisión de un delito del que pueda seguirse con probabilidad la muerte o una lesión física grave de una persona (...) y a efectos de investigación de un delito penal grave*"[31].

Seguindo tais coordenadas, a Convenção sobre o Cibercrime (Budapeste, 23 de novembro de 2001) veio finalmente a reconhecer tal possibilidade, ainda que com certos limites, tendo em vista que o seu art. 32° autoriza os acessos transfronteiriços a dados armazenados, mas somente quando se trata de dados informáticos armazenados de livre acesso ao público (fonte aberta) ou com o consentimento legal e voluntário da pessoa autorizada para divulgá-los através do sistema informático visado.[32]

Contudo, o regime internacional existente se mostrou inadequado e insuficiente, de modo que muitos países passaram a incorporar dentro do catálogo de medidas legais de investigação criminal, de maneira unilateral, certas medidas de alcance extraterritorial. Em Portugal, a Lei do Cibercrime (109/2009), no seu art. 19°, possibilita estender o registro de um equipamento informático a outros sistemas que resultem acessíveis através do equipamento inicialmente examinado, quando existem motivos suficientes para crer que os dados solicitados se encontram nesse outro sistema, não existindo qualquer limitação territorial no referido art. 19°, parecendo-nos ser possível tal medida mesmo que o outro sistema encontra-se em território estrangeiro.[33]

Por outro lado, mas ainda quanto as peculiaridades da obtenção da prova em ambiente digital, devemos ter em mente que além dos princípios genéricos vigentes em matéria de processo penal ao nível de prova, a obtenção da prova forense digital implica o reconhecimento e aplicação de princípios específicos que estão ligados as mencionadas características desse tipo de prova. Entre eles, podemos citar o princípio da não alteração da prova eletrônico-digital, que segundo Rodrigues (2009), exige um maior esforço por parte do investigador forense digital, para que o mesmo, desde o momento da recolha dos vestígios, até a posterior apresentação dos resultados, não insira variações ou contamine os dados com elementos estranhos ao próprio sistema ou rede informáticos sob investigação.[34]

---

[31] Posição Comum 1999/364/JAI, de 27 de maio de 1999, relativa ás negociações do projeto de Convenio sobre o Cibercrime.
[32] PRADILLO, Juan Carlos Ortiz. *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, 2013, p. 16.
[33] *Ibidem.*
[34] RODRIGUES, Benjamim Silva, 2009, p. 576-578.

Outro princípio de especial importância citado pelo autor, é o princípio da especialização ou qualificação do pessoal adstrito à investigação forense digital. Desta forma, o acesso, recolha, conservação e análise da prova forense tem de ser levada a cabo por pessoal especializado, com conhecimentos técnico-científicos, sob pena da mesma não ser corretamente manuseada e para sempre perdida para o processo penal em vista da sua inadmissibilidade. Entre outros, há também que se mencionar o princípio da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação da prova eletrônico-digital, com o objetivo de manter a cadeia de controle da mesma.[35]

Atualmente, em Portugal, a prova digital e sua respectiva obtenção está regulada em três diplomas legais diferentes: o Código de Processo Penal; a Lei nº 32/2008, de 17 de julho (que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas); e a Lei nº 109/2009, de 15 de setembro (Lei do Cibercrime), que prevê disposições processuais aplicáveis a crimes informáticos, crimes cometidos por meio de um sistema informático e, quaisquer crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrônico.[36]

A doutrina muito tem criticado o fato do legislador nacional continuar a manter em vigor três diplomas legais diferentes para regular aspectos parcelares da mesma realidade concreta, o que acentua o atual modelo da descodificação e nega a desejável centralidade normativa do Código de Processo Penal, contribuindo para a assimetria, para a incoerência das soluções legais e, sobretudo, para o indesejável e nefasto insucesso prático. Nesse sentido, Correia entende que "a prova digital – essencial no mundo hodierno – continua mergulhada num verdadeiro pântano prático e, sobretudo, normativo, que só poderá ser superado mediante uma intervenção legislativa coerente, global e, cientificamente, sustentável".[37]

Essa problemática existente entre o desenvolvimento tecnológico e o processo penal é também muito bem exposta por Figueiredo Dias, quando afirma que entre

[35] *Ibidem.*

[36] Ou seja, em razão do art. 11º, nº 1, al. c), a Lei do Cibercrime compreende um regime geral sobre recolha de prova em suporte eletrônico aplicável a quaisquer crimes, pelo que as regras processuais são aplicáveis de uma forma geral a um universo de crimes aberto, independente dos elementos típicos.

[37] CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter, in: Revista do Ministério Público, ano 35, nº 139, Lisboa, 2014, p. 30.

> "os novos âmbitos problemáticos que se colocaram à legislação e à ciência do processo penal nos últimos tempos [...] o primeiro tem que ver com a circunstância de os novos horizontes técnico-científicos terem aberto a porta a métodos de investigação até há não muito tempo desconhecidos".[38]

O autor continua, referindo que nesse aspecto

> "se incluem, entre outros, os métodos de investigação computadorizados ou, de forma mais geral, permitidos pelos avanços informáticos (nomeadamente, a confrontação de dados e a criação de apertadas redes de informação), a aparição de formas de vigilância e de registro de voz e de imagem através de câmaras ou de sofisticados aparelhos de escuta e de gravação, [...]"[39].

E justamente devido à essas complexidades criminalísticas impostas pelo avanço tecnológico, resultando nas peculiaridades e dificuldades da obtenção da prova digital, o Estado, na obrigação de salvaguardar a segurança dos seus cidadãos, se viu na necessidade de uma equiparação de armas, utilizando-se de tecnologias que até então eram empregadas apenas para fins ilícitos e por *hackers*[40], para que então pudesse combater e rastrear os autores desses crimes em âmbito digital, bem como para recolher provas digitais eventualmente deixadas por crimes praticados no mundo material. Estamos falando da utilização de métodos ocultos de investigação para obtenção de prova em ambiente digital.

[38] DIAS, Jorge Figueiredo. O processo penal português: problemas e perspectivas, in AA.VV, Que futuro para o direito processual penal? – Simpósio em homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal português, Coimbra: Editora Coimbra, 2009, p. 808-809.
[39] *Ibidem.*
[40] Nesse sentido, Mata-Mouros afirma que "fruto das incessantes inovações tecnológicas, estes métodos de investigação não cessam de se multiplicar, numa dinâmica que invariavelmente tem como primeiros utilizadores os próprios agentes criminosos, para só de seguida motivar agentes policiais e, apenas no fim da cadeia, encontrarem expressão na legislação e no aplicador do direito". MATA-MOUROS, Maria de Fátima. Juiz das Liberdades – Desconstrução de um Mito do Processo Penal, Coimbra: Almedina, 2011, p. 433.

## 2. As medidas antiforenses

Antes de tratarmos sobre os métodos ocultos de investigação criminal, iremos tratar sobre as *medidas antiforenses*, que se mostram como a maior justificativa para a utilização dos métodos ocultos em ambiente digital, já que tornam a obtenção da prova digital mais difícil do que já é.

Devido ao sucesso de investigações como a do *Silk Road*, e devido a evolução da Ciência Forense Digital e da crescente intromissão estatal no conteúdo das telecomunicações, tem sido desenvolvido programas informáticos com o intuito de frustrar a detecção, monitorização, prova ou imputação de uma determinada atividade online ao seu autor: são as chamadas medidas antiforenses ou contraforenses.[41]

Segundo Ryan Harris, as medidas antiforenses são

> "quaisquer tentativas de comprometer a disponibilidade ou utilidade da prova no processo forense. Comprometer a disponibilidade da prova inclui quaisquer tentativas de evitar que a prova venha a existir, de esconder prova existente ou de manipular a prova no sentido de assegurar que a mesma deixe de estar ao alcance do utilizador. A utilidade pode ser comprometida através da obliteração da própria prova ou da destruição da sua integridade"[42].

Ou, de uma maneira mais sucinta, nas palavras de Scott Berinato: "*Make it hard for them to find you and impossible for them to prove they found you*"[43].

Nesse sentido, pode-se dizer que o objetivo das várias medidas antiforenses utilizadas pelos criminosos que praticam ilícitos por meio de sistemas informáticos (ou que os utilizam para se comunicar e arquitetar planos) é o de frustrar a referida Ciência Forense Digital e o seu respectivo intuito de obter a prova digital capaz de incriminá-los. Mas antes mesmo de pretender frustrar que a entidade investigadora tenha acesso aos dados informáticos com valor probatória contra o visado, o esforço deste incide, primeiramente, na ocultação do seu rastro digital e, consequentemente, da sua

[41] RAMALHO, David Silva, 2017, p. 150-151.
[42]HARRIS, Ryan. *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensic sproblem, Digital Investigation - The international Journal of Digital Forensics & Incident Response*, Vol. 03 – Suplemento, 2006, p. 45.
[43]BERINATO, Scoot. *The Rise of Anti-Forensics*, CSO Online, 2007. Disponível em: http://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html. Acesso em: 18/04/2016.

identidade.[44] A seguir descrevemos os diferentes tipos de medidas antiforenses, segundo David Silva Ramalho.[45]

*a) Anonimizadores*

Uma das medidas frequentemente utilizada para frustrar as investigações criminais em ambiente digital são os *softwares* de anonimização, que visam impedir que o investigador criminal consiga associar uma certa conduta online ao seu autor, frustrando o objetivo de identificar o sistema informático inicial, fazendo isso por meio de servidores *proxy, mix cascades* ou *onion routing*.[46]

O servidor *proxy* (em especial o servidor *proxy* baseado na *web*) funciona como um intermediário entre o utilizador e a página visada que envia o tráfego da Internet, escondendo o endereço IP do sistema informático do utilizador. Para Osvaldo Santos, o servidor *proxy* ou *gateway* aplicacional é

> "um dispositivo ou sofware que atua em nome dos seus clientes relativamente a um determinado serviço. Os clientes fazem os pedidos ao servidor *proxy* e é este que realmente interage com os servidores de destino para obter as respostas aos pedidos efetuados pelos clientes. Quando as respostas chegam ao servidor *proxy*, este devolve-as aos clientes que fizeram os respectivos pedidos"[47].

Apesar de existirem diversos tipos de servidores *proxy* com diferentes graus de segurança e finalidades, os mesmos não proporcionam um anonimato total, pois ainda que proporcionem o anonimato do utilizador perante o sistema informático, o mesmo não se aplica para o próprio servidor *proxy*, que consegue identificar o sistema informático do utilizador[48], de modo que poderá ser forçado a revelar essa informação caso requerido pela autoridade competente.

Em razão disso, sugiram as *mixcascades*, que são um sistema de *proxies* em cadeia que fazem com que o mesmo *proxy* receba comunicações de várias origens diferentes, misturando-as antes de enviar a informação para outro *proxy* aleatório,

[44] RAMALHO, David Silva, 2017, p. 152.
[45] *Idem*, p. 150-175.
[46] *Idem*, p. 153.
[47] SANTOS, Osvaldo. *Firewalls – Soluções práticas*, Lisboa: FCA – Editora de Informática, 2011, p. 62.
[48] WEBER, Rolph e HEINRICH, Ulrike I., *Anonymization*, Londres: Springer, 2012, p. 17.

repetindo esse processo até chegar ao destinatário final[49], o que confere um maior grau de anonimato ao utilizador do que o servidor *proxy* normal. Já as referidas *onion routing* tem o objetivo de garantir a confidencialidade e inviolabilidade das comunicações dos seus utilizadores, além do anonimato do seu remente, sendo que o programa mais utilizado nesta matéria para a prática de ilícitos é o já referido TOR, que funciona com base no envio da comunicação por um sistema de roteamento, passando por distintos pontos sob diferentes camadas de cifragem até chegar ao seu destinatário.[50]

*b) Moedas virtuais: bitcoin*

Outro mecanismo que merece ser destacado como uma forma de dificultar a obtenção da identidade dos usuários e, consequentemente, de provas contra os mesmos na eventualidade de uma investigação criminal, são as chamadas moedas virtuais. Não é de hoje que indivíduos se esforçam com intenções de atuar contra os riscos para a privacidade provocado pelas novas tecnologias, bem como contra os poderes do sistema financeiro e o seu modo de exercício, entendidos genericamente como contrários aos interesses do cidadão comum. Segundo Ramalho, um dos meios que triunfou para atingir tais objetivos foi a criação de uma moeda virtual, independente de quaisquer entidades centralizadas, possibilitando conduzir transações anônimas, paralelas ao sistema instalado e habitualmente sem comissões.[51]

Nesse segmento, merece especial destaque a *bitcoin,* tendo em vista ser a moeda digital mais conhecida e utilizada (ainda que existam outras moedas virtuais, trataremos apenas da *bitcoin*, e de maneira breve, evitando exaustiva tecnicidade, tendo em vista a complexidade da matéria para um jurista).

Criada em 2008 por Satoshi Nakamoto (cuja verdadeira identidade permanece desconhecida), pode ser considerada como um sistema de pagamento eletrônico tendencialmente anônimo, descentralizado e inteiramente virtual, de troca, em modo *peer-to-peer* (ou seja, diretamente entre os usuários e sem intervenção de outras entidades ou terceiros de confiança), de unidades monetárias geradas pela rede, cujo valor é fixado pela oferta e procura, e que são armazenadas nas carteiras digitais

[49] BETTINI, Claudio. *et al., Privacy in Location-Based Applications: Research Issues and Emerging Trends,* Berlim/Heidebelg/ Nova Iorque: Springer, 2009, p. 88.
[50] RAMALHO, David Silva. O uso de *malware* como meio de obtenção de prova em processo penal, in Revista de concorrência e regulação, Lisboa, Ano 4, nº 16, 2013, p. 210.
[51] VIGNA, Paul e CASEY, Michael J., *The age of Cryptocurrency – How Bitcoin and Digital Money are challenging the Global Economic Order,* Nova Iorque: St. Martin's Press, 2015, p. 48-52.

(*digital wallets*) dos seus utilizadores. Dessa forma, por meio da instalação de um *software* gratuito e de *open source* (código aberto), os utilizadores do sistema *bitcoin* podem enviar e receber *bitcoins* entre si através da aposição de sucessivas assinaturas digitais, de forma potencialmente indetectável, tendencialmente sem quaisquer comissões, de forma rápida para qualquer parte do mundo.[52]

Ademais das diversas peculiaridades inerentes à *bitcoin* e à sua criação e funcionamento[53], a importância da mesma para o presente trabalho, em específico para a investigação criminal, é a dificuldade que a mesma trouxe para o sucesso de uma das regras basilares da investigação criminal, conhecida pela expressão "*follow the money*". Tendo em vista que a prática de ilícitos criminais geralmente tem como objetivo a obtenção de um ganho patrimonial, na maioria das vezes de natureza pecuniária, a procura do rastro do dinheiro, segundo Blakeslee, é uma das vias utilizadas para ligar a conduta ilícita ao seu autor, superando elementos de dissimulação utilizados.[54] Dessa maneira, a utilização de elementos anonimizadores ou outras medidas antiforenses poderão revelar-se inúteis se, ao final da conduta ilícita, a recompensa tiver de ser transferida de forma identificável para uma conta bancária titulada pelo autor do ilícito sob investigação.[55]

É em razão disso que é recorrente a criação de novos e mais complexos esquemas de transferência de capitais com o objetivo de possibilitar que os lucros da atividade ilícita cheguem ao seu beneficiário sem serem detectados pelos órgãos de policia criminal. Assim, ainda que a criação das novas moedas virtuais não tenha quaisquer intentos de cariz criminoso, acabou por ser rapidamente aproveitada para suprir as fragilidades da transferência regular de capitais de origem ilícita. É nesse sentido que Ramalho conclui que

> "as técnicas anonimizadoras para condução de actividades criminosas *online*, juntou-se a obtenção de proventos monetários de forma potencialmente indetectável, com recurso a um novo mecanismo que, em geral, permanece por regular"[56].

[52]BASU, Sonal *et al., Bitcoin – Bubble or Reality?, Computer Law Review international*, Vol. 15, nº 3 (Junho 2014), pp. 73-740, *apud* RAMALHO, David Silva, 2017, p. 160-161.
[53] Para maiores informações sobre a moeda virtual *bitcoin*, ver: NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer electronic cash system*, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 23/04/2017.
[54] BLAKESLEE, Melise R., *Internet Crimes, Torts and Scams – Investigation and Remedies*, Oxford: Oxford University Press, 2010, p. 6-7.
[55] RAMALHO, David Silva, 2017, p. 164.
[56] *Ibidem*.

*c) Medidas antiforenses que visam evitar o exame e análise de dados informáticos*

Superada a fase de identificação do autor do ilícito e/ou do sistema informático utilizado para a prática do mesmo, no qual se encontram armazenadas informações relevantes para a investigação e/ou a partir do qual a mesma pode ser acessível, chega o momento de proceder a sua recolha, exame e análise. É por meio deste processo que os dados informáticos são processualmente convertidos em prova digital e passam a servir de suporte a uma tese que tendencialmente virá a ser judicialmente testada. Contudo, atualmente, qualquer utilizador que tenha conhecimentos mínimos em tecnologias de informação pode ter acesso a instrumentos de proteção da informação em suporte digital, onde facilmente poderá eliminar de forma irreversível os elementos incriminatórios contra si, ou instalar no seu sistema informático as medidas necessárias para a dissimulação dos dados ou a sua adulteração para efeitos de contaminação da prova recolhida.[57]

Entre as medidas antiroferenses utilizadas com intuito de frustrar a atividade de recolha da prova, destacam-se a eliminação de dados (*data wiping),* a esteganografia, a cifragem de dados, e a adulteração de dados.[58]

A eliminação de dados ou limpeza do disco trata-se, de acordo com Domingues, da eliminação definitiva dos dados armazenados em um determinado sistema informático. Quando um ficheiro/arquivo é eliminado do disco rígido, o sistema não o extingue completa e irreversivelmente de imediato, mas geralmente limita-se a remover o apontador a esse ficheiro, tornando-o invisível, tendo em vista que a eliminação definitiva dos dados requer um esforço de processamento desnecessário para o sistema e é prejudicial ao seu rendimento. Assim, enquanto novos ficheiros não ocuparem o espaço marcado como livre onde "jazem" os ficheiros que se visava eliminar, estes permanecerão no sistema.[59]

É em razão disso que mesmo depois da eliminação dos dados, um perito forense pode reavê-los total ou parcialmente caso não tenham sido substituídos por outros dados. Assim, é cada vez mais frequente a utilização de ferramentas de *data wiping* (programas como, por exemplo, o *Eraser* e o *CCleaner*), visando tornar irrecuperáveis os arquivos eliminados de um sistema informático através da substituição

[57] *Idem*, p. 165.
[58] *Idem,* p. 165-173.
[59] DOMÍNGUES, Francisco Lázaro. *Introducción a la informática Forense,* Madrid: Ra-Ma, 2013, p. 68.

por uns, zeros ou caracteres aleatórios. Ramalho lembra que em determinados casos a eliminação definitiva dos ficheiros pode ser feita por via remota, com recurso a *remote "kill" switches*, ou por intermédio da destruição física dos suportes físicos nos quais se encontram armazenados, seja pela incineração, corrosão com ácido ou desmagnetização com uso de ímanes.[60]

Esse procedimento é frequentemente utilizado após a descoberta ou mera suspeita, por parte dos perpetradores de ilícitos criminais, da existência de uma investigação criminal em curso. Inclusive, há relatos de um *software* chamado *Panic Button*, geralmente utilizado por consumidores de pornografia infantil na Internet, que efetua esse procedimento de eliminação definitiva dos dados em caso de suspeita da iminência de uma investigação policial ao sistema informático no qual os dados encontram-se armazenados.[61]

Outras medidas antiforenses que merecem destaque são aquelas que visam a dissimulação de dados. Geralmente, quando o visado não suspeita que os seus dados informáticos estão na mira de uma investigação criminal, ele os manterá na sua posse, seja no próprio sistema informático ou em suportes removíveis (*pen drives*, CDs, DVDs, etc.). Todavia, e principalmente quando se está diante de informações com elevado valor probatório na posse de indivíduos cautelosos e tecnologicamente letrados, é comum que tal informação seja dissimulada por mecanismos que tornam sua detecção e obtenção muito difícil. Entre essas técnicas, as mais conhecidas são a criptografia e a esteganografia.[62]

A cifragem de dados permite ao seu utilizador tornar certo ficheiro em um criptograma, o que torna o seu acesso potencialmente impossível para quem não tenha a respectiva chave de desencriptação, tornando o conteúdo ilegível a terceiros. Kerr chama atenção que em certos casos, dependendo do tipo de chave utilizado, da palavra-passe utilizada para a cifragem, e do *software* de decifragem utilizado, a tentativa de decifrar os dados sem conhecimento da chave inicial pode levar alguns segundos ou milhares de anos, tornando praticamente impossível o sucesso de uma investigação criminal.[63]

---

[60] RAMALHO, David Silva, 2017, p. 166-167.
[61] RAMALHO, David Silva, 2013, p. 211.
[62] RAMALHO, David Silva, 2017, p. 167.
[63] KERR, Orin S., "*The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?*", 33 *Connecticut Law Review 503,* Vol. 33, 2001, p. 503-504. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=927973.

Como se não bastasse, tem se aumentado o uso de ferramentas de encriptação completa do disco, onde não é apenas um ficheiro que é criptografado, mas todo o disco rígido de um sistema informático ou de um dispositivo removível é sujeito a encriptação, tornando teoricamente irrecuperável toda a informação armazenada. Pois se a encriptação de ficheiros específicos pode ser contornada pela procura de pistas deixadas por descuido no sistema informático do visado, tornando possível sua descoberta, a encriptação completa do disco torna isso incontornável, sendo imprescindível o uso da palavra chave.[64]

Esse caráter inultrapassável da encriptação fez com que países como os EUA, Reino Unido e França, criassem tentativas de regular a pesquisa sobre desenvolvimento de tecnologias de encriptação e utilização de encriptação em comunicação.[65] Todavia, tais restrições não prosperaram, tendo em vista o domínio sem fronteiras que é a Internet, tornando, em certos casos, necessária a encriptação em setores-chave e na comunicação eletrônica em geral. Da mesma maneira, fracassaram as tentativas de imposição da criação de *backdoors* (vulnerabilidades intencionalmente colocadas) em sistemas de encriptação acessíveis ao público com o intuito de permitir ao Estado contorná-los caso necessário. Tal frustração ocorreu em razão de as *backdoors* trazerem fragilidades passiveis de serem aproveitadas por terceiros mal-intencionados e por frustrar-se o propósito de obtenção de privacidade face ao próprio Estado que em muitos casos motivava a utilização da encriptação.[66]

Mas a utilização de encriptação não significa uma completa impossibilidade de descoberta do conteúdo encriptado. Além das técnicas para decifrar os ficheiros visados, que geralmente obtêm sucesso nos casos em que a palavra-chave é fraca, existe também a possibilidade de impor a revelação de dados quando os mesmos sejam cifrados por uma entidade terceira, que os detém. Nesses casos, com base no disposto no artigo 14º da Lei do Cibercrime, a chave pode ser obtida por meio de uma injunção para apresentação ou concessão do acesso a dados.[67] Sobre a injunção, Pedro Verdelho refere que:

> "as razões subjacentes a este mecanismo relacionam-se com a incomensurável capacidade de armazenamento de dados dos sistemas informáticos modernos, que muitas vezes inviabilizam a obtenção de conteúdos neles guardados. Por via da injunção criou-se uma forma de os

[64] RAMALHO, David Silva, 2017, p. 168.
[65] Sobre isso, ver: ROWLAND, Diane. et al., *Information Technology Law*, 4.ª Ed. Nova Iorque: Routledge, 2012, p. 224-225.
[66] RAMALHO, David Silva, 2017, p. 169.
[67] *Idem*, p. 170.

> obter compulsivamente, mesmo que tais conteúdos estejam ocultos no sistema, encriptados ou protegidos por *passwords".*[68]

Todavia, nos casos em que apenas o arguido possua a informação para a decifragem dos dados, e mesmo que eles estejam armazenados a cargo de uma terceira entidade que forneça a cifragem mas não possua a chave para decifragem, a chave não poderá ser obtida por meio da imposição coativa da sua revelação, tendo em vista o disposto no artigo 14º, nº 5, da Lei do Cibercrime, devendo o investigado ser informado da possibilidade legal de recusa, não podendo ser obrigado a produzir prova contra si mesmo[69], de modo que um dos únicos mecanismos que se mostrará útil na obtenção desses dados será a utilização de *malware* por parte dos investigadores criminais, o que será abordado mais a frente.

Por outro lado, outra técnica de dissimulação de dados utilizada com frequência é a esteganografia. Com o uso dela, é possível esconder em um ficheiro de áudio, de imagem ou de vídeo aparentemente inofensivos, outras mensagens, imagens ou conteúdo audiovisual de aspecto potencialmente ilegal, que poderiam ser usados como prova contra o visado. Ao ponto que a encriptação torna um ficheiro indecifrável sem a palavra-chave correta, mas permite a um investigador saber a existência desse ficheiro e a intenção de tornar seu conteúdo inacessível a terceiros, a esteganografia permite esconder um ficheiro dentro de outro aparentemente inofensivo, de modo que a mera detecção deste tipo de ficheiro se mostra problemática, podendo facilmente ser ignorado por aparentar ser irrelevante.[70] Importante ainda trazer Cole, quando o autor destaca que para elevar a dificuldade na descoberta de informações, ambas às tecnologias de encriptação e esteganografia podem ser cumuladas, fazendo primeiro a encriptação de um ficheiro e após a sua dissimulação dentro de outro ficheiro aparentemente inofensivo[71].

É nesse sentido que se pode afirmar que apenas uma investigação criminal rigorosa e atenta poderá detectar os elementos probatórios quando tais técnicas de

---

[68] VERDELHO, Pedro. "Lei do Cibercrime", em AA.VV., *Enciclopédia de Direito e Segurança* (coord. Jorge Bacelar Gouveia e Sofia Santos), Coimbra: Almedina, 2015, p. 262.

[69] RAMALHO, David Silva, 2017, p. 170. E também, sobre isso, ver: PINTO, Lara Sofia. "Privilégio contra a auto-incriminação versus colaboração do arguido. *Case study:* revelação da *password* para desencriptação de dados – *resistance is futile?*", em Prova Criminal e Direito de Defesa. Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal (coord. Teresa Pizarro Beleza/Frederico de Larcerda da Costa Pinto), Coimbra: Almedina, 2013, p. 91-116.

[70] RAMALHO, David Silva, 2017, p. 170-171.

[71] COLE, Eric. *Hiding in plainsight: Steganography and the Art of Covert Communication*, Indiana: Wiley Publishing, 2003, p. 5.

dissimulação forem utilizadas, e quanto mais a tecnologia evolui e a preocupação com a privacidade e confidencialidade das comunicações vai aumentando, mais comum e acessível se torna o uso de tais ferramentas de dissimulação.[72]

Por fim, importante mencionar também os mecanismos utilizados para adulteração de dados, onde os dados informáticos se mostram já intencionalmente contaminados no momento da recolha, justamente para frustrar a sua detecção ou sua utilidade como prova. Entre esses programas, destaca-se o *Timestomp*, cuja principal função é alterar o *metadata* que registra a data de criação e de alteração de ficheiros[73]. Dessa forma, como destaca Ramalho, se um investigador usar como um dos parâmetros de pesquisa a data de criação ou de adulteração dos documentos visados, o resultado encontrado poderá não incluir a prova que realmente se pretende obter, por ter a mesma sofrido previa alteração nessas propriedades. Existem também programas que modificam as extensões e assinaturas dos documentos informáticos, permitindo que certos documentos pareçam ser de tipo diferente. Por exemplo, o suspeito pode fazer um arquivo de vídeo se passar por um arquivo executável (.exe), de modo que se o investigador está buscando por um vídeo, não o encontrará com facilidade, o que é utilizado com frequência por indivíduos suspeitos de pornografia infantil.[74]

Mas devemos ter em mente que o impacto desta e das outras técnicas mencionadas aqui (a eliminação de dados, a esteganografia e a encriptação), será inferior para uma investigação criminal do que as técnicas de anonimização e de utilização de moedas virtuais. Isto pelo fato de que a eliminação, dissimulação ou alteração de dados compromete, regularmente, a disponibilidade desses dados, ao ponto que as ferramentas para evitar detecção não impedem a regular utilização do sistema e redes informáticas por parte do individuo. Dessa forma, se o investigado não suspeita da existência de uma investigação criminal, e essa for realizada com apreensões rápidas do material informático probatório, essas técnicas dificilmente serão aptas a bloquear ou fragilizar a investigação. Todavia, serão de grande utilidade para o suspeito se ele for extremamente cauteloso e, sempre que esteja sem contato direto e imediato com o seu

[72] RAMALHO, David Silva, 2017, p. 171.
[73]SCHAFER, Burkhard e MASON, Stephen. "*The characteristics of electronic evidence in digital format*", em AA.VV., *Eletronic Evidente(*Stephen Maison*),* Londres: Lexis Nexis Butterwoths, 2012, p. 53.
[74] RAMALHO, David Silva. 2017, p. 172-173.

sistema informático, utilize uma ou varias dessas técnicas que visam evitar o exame e análise dos seus dados informáticos.[75]

*d) Ataques contra pericias forenses*

Como última medida antiforense, há que se referir os ataques contra perícias forenses, onde determinado *software* preventivamente instalado no sistema informático do investigado, ao detectar a iminência de uma perícia, ativa mecanismos de agressão ás próprias ferramentas com que se efetuam as perícias, falsificando ou modificando a prova e tornando-a ilegítima em sede judicial. Esses *softwares* geralmente se beneficiam do fato de muitos dos programas utilizados pelas autoridades investigativas para recolha da prova digital terem, por uma questão de transparência, o seu código-fonte livremente acessível (*open source)*, tornando possível explorar suas vulnerabilidades.[76]

Portanto, com o exposto até aqui é possível concluir que as novas tecnologias, além de tornar mais fácil a prática de ilícitos criminais em ambiente digital, ao mesmo tempo tornaram mais difícil a sua detecção e, principalmente, a obtenção da prova da sua prática. Dessa maneira, em razão da multiplicação das medidas antiforenses referidas acima e de muitas outras, e da facilidade com que elas podem ser adquiridas e utilizadas por usuários com conhecimentos técnicos medianos, se mostra de suma importância a utilização e instalação de métodos ocultos de obtenção de prova no computador visado para a obtenção de prova quando a gravidade do caso assim o justifique, como veremos a frente.[77]

[75]*Idem,* p. 173.
[76] *Idem,* p. 174.
[77]PRADILLO, Juan Carlos Ortiz, *Problemas procesales de La Ciberdelincuencia*, Madrid: Editorial Colex, 2009, p. 177-178.

# II. MÉTODOS OCULTOS DE INVESTIGAÇÃO E A BUSCA DA VERDADE NO PROCESSO PENAL

Por métodos ocultos de investigação criminal, entende-se como

> "todos aqueles métodos que representam uma intromissão nos processos de acção, interacção, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência ou disso sequer se apercebam".[78]

Dessa forma, as pessoas atingidas pela medida (geralmente o suspeito) continuam a se comunicar, agir e expressar de forma "inocente", fazendo ou dizendo coisas totalmente autoincriminatórias (ou incriminatórias das pessoas com quem se comunicam), motivo pelo qual é possível afirmar que os métodos ocultos de investigação levam os atingidos a ditar inconscientemente para o processo "confissões" não esclarecidas nem livres (como o método oculto mais conhecido, podem-se citar as escutas telefônicas).[79] É nesse sentido que Ramalho afirma que os métodos ocultos

> "assumem, por isso, como principal elemento caracterizador a imposição secreta de uma neutralização casuística de direito fundamentais e garantias processuais do visado, ou mesmo da criação de um *estado de exepção* a certos princípios gerais do processo penal, em prol da eficácia na realização da Justiça".[80]

O secretismo dos métodos ocultos se mostra fundamental para sua eficácia, e a utilização cada vez mais frequente desse recurso se mostra mais do que mero agravamento da ação repressiva do Estado, mas sim uma verdadeira modificação da tradição clássica do processo penal, fundado na colaboração involuntária e desinformada do suspeito para que produza prova contra si da sua própria conduta criminosa.[81]

Portanto, pode-se dizer que os métodos ocultos de investigação sacrificam um conjunto de bens jurídicos e direitos fundamentais como a privacidade/intimidade, palavra, imagem, sigilo profissional, inviolabilidade do domicílio, sigilo das telecomunicações, confidencialidade e integridade dos sistemas técnico-informacionais, e autodeterminação informacional. Além disso, os meios ocultos também sacrificam o

[78] ANDRADE, Manuel da Costa, 2009, p. 105.
[79] *Ibidem.*
[80] RAMALHO, David Silva, 2017, p. 34.
[81] *Ibidem.*

direito a recusar testemunho ou depoimento, o princípio *nemo tenetur se ipsum accusare*, e o direito ao silencio.[82]

É em razão disso, que para o direito positivo, o simples fato de um método de investigação criminal ser configurado como oculto, não permite sua simples integração em um *sistema*, bem como não garante uma conclusão fácil pela sua aplicação, tendo em vista que não existe uma teoria geral reguladora desta matéria no ordenamento jurídico português, sendo a mesma tratada de maneira esparsa e desprovida de unidade dogmática.[83]

Os diplomas extravagantes prevendo métodos ocultos de investigação criminal surgem autonomamente e conforme as necessidades de investigação ou de política criminal, permanecendo distantes do Código de Processo Penal, de modo que Costa Andrade afirma que

> "tomado no seu conjunto, o direito português dos meios ocultos de investigação caracteriza-se pelas lacunas e descontinuidades, incongruências e inconsistências e, sobretudo, por insustentáveis contradições e assimetrias normativas, axiológicas e político-criminais".[84]

Por outro lado, devemos ter consciência de que os métodos ocultos de investigação vieram para ficar, tornando-se insubstituíveis na perseguição e repressão de uma nova fenomenologia criminal (como por exemplo, a criminalidade organizada e trasnacional) onde os meios tradicionais e "abertos" de investigação se mostram ineficazes e incapazes de obter as provas necessárias para combater tal criminalidade (sem falar nos ilícitos praticados em ambiente digital, onde a obtenção de prova se mostra mais complicada, não só pelas questões técnicas vistas, mas também em razão de as transformações científico-tecnológicas caminharem mais rápidas que as jurídico-políticas). E por mais que não representem um dado inteiramente novo na experiência processual penal, foram nas duas últimas décadas que os métodos ocultos apareceram com força e se instalaram definitivamente no processo penal. Isso se deu, principalmente, por duas linhas de força: de um lado, o triunfo da ideologia de *war on terrorism*, vinda com força a partir dos Estados Unidos; e do outro lado, em razão das profundas e estruturais transformações trazidas pelos progressos tecnológicos no domínio das telecomunicações. Isso tudo seguindo o modelo das escutas telefônicas, o

[82] ANDRADE, Manuel da Costa, 2009, p. 106-107.
[83] RAMALHO, David Silva, 2017, p. 34-35.
[84] ANDRADE, Manuel da Costa, 2009, p. 109.

primeiro método oculto institucionalizado, o qual trouxe triunfo para esta categoria de métodos de investigação.[85]

Todavia, é inegável a drástica e comprometedora danosidade social que os métodos ocultos trazem consigo. Para além dos bens jurídicos e direitos fundamentais que atingem, como anteriormente mencionado e que posteriormente serão analisados com maior rigor, os métodos ocultos têm também a tendência para invadir a esfera jurídica de um número incontrolável de pessoas, não distinguindo suspeito e inocente, não respeitando relações de confiança, de segredo, e de proximidade existencial. Vale citar um caso da Alemanha, onde em janeiro de 2007 foi informado que para elucidação de um caso de pornografia infantil na Internet, foram inspecionados todos os cartões de crédito na Alemanha (mais de vinte e dois milhões).[86] Um caso assim se aproxima perigosamente das visões de George Orwell no seu livro 1984.

Como outra consequência do uso dos métodos ocultos, Costa Andrade afirma que

> "o centro de gravidade das decisões tende a deslocar-se do julgamento (público) para os resultados das investigações ocultas. Se o julgamento tende a transformar-se num ritual externo, a figura e a função do juiz ficam cada vez mais desarmadas e debilitadas em benefício do Ministério Público e, sobretudo, da polícia. Enquanto isso, também o arguido vê minado o seu estatuto de *sujeito processual*, aproximando-se progressivamente de um mero objecto do processo".[87]

O autor continua, demonstrando que outra questão que merece destaque é o fato de que por não terem conhecimento da medida antes e durante sua execução, as pessoas atingidas não poderão propor qualquer pretensão de reação e tutela, mesmo que legalmente subsistente e consignada. Diferentemente de outras medidas de coação, como a prisão preventiva por exemplo, que a qualquer momento pode ser contestada, infirmada e neutralizada, quando se está diante de um método oculto, a pessoa não pode, concretamente, fazer valer a ilegalidade da medida por violação de qualquer dos pressupostos legais. Isso se deve justamente pelo fato de que a pessoa atingida só toma conhecimento (se toma) depois de a medida ter ocorrido, sendo tarde demais, já que a medida já terá irreversivelmente desencadeado seu potencial de devassa.[88]

---

[85] *Idem*, p. 109-111.
[86] ROXIN, Claus. *La prohibición de autoincrinación y de las escuchas domiciliares*¸apresentação de Francisco Muñoz Conde e Marcela De Langhe, Buenos Aires: Hammurabi, 2008, p. 47.
[87] ANDRADE, Manuel da Costa, 2009, p. 107.
[88] *Ibidem.*

Ainda, a medida já terá reforçado a existência dos pressupostos que devem ser cumpridos no momento de sua imposição (como veremos adiante), os quais poderiam em um primeiro momento, revelar-se insuficientes e problemáticos. A título de exemplo dessa problemática, com muita maestria expõe Costa Andrade:

> "a generalidade destas medidas integram entre os seus pressupostos um determinado grau de *suspeita* da prática de um crime (do catálogo). Com que hipóteses de sucesso e com que eficácia pode um arguido vir invocar que, ao tempo em que a medida foi ordenada ou autorizada, não existia a suspeita reclamada e pressuposta pela lei se, entretanto, já a medida aumentou, ela própria, a plausibilidade da suspeita, convertendo-a numa 'certeza'?"[89].

Portanto, é em razão das problemáticas expostas acima, e do que será exposto adiante, que é inegável a necessidade de criar uma ordem no caos normativo em que os métodos ocultos se encontram. Diferentemente do que ocorre na Alemanha, onde foram chamados todos os métodos ocultos de investigação ao Código de Processo Penal e passou a se estabelecer um *sistema*, em Portugal os mesmos se encontram dispersos por diferentes diplomas, pois enquanto uns estão regulados no Código de Processo Penal (como as escutas telefônicas), outros estão dispersos por diplomas extravagantes (como os agentes encobertos, Lei nº 101/2001; os registros fotográficos, Lei nº 5/2002; a vídeo vigilância, Lei nº 1/2005; ou, a mais recente, os métodos ocultos de investigação em ambiente digital previstos na Lei nº 109/2009, de 15 de setembro). E também, há aqueles que ainda não conheceram sancionamento legal e vão sendo utilizados na margem da ilegalidade.

Contudo, antes de tratarmos sobre os métodos ocultos mais utilizados para obtenção de prova em ambiente digital, e sobre a maneira que se entende que o legislador deveria prever tal matéria, devemos tratar sobre a descoberta da verdade no processo penal e as proibições de prova, temas diretamente ligados com a matéria em análise.

## 1. A descoberta da verdade no processo penal

O processo penal, durante décadas passadas, era regido pelo princípio da verdade material (também chamado de verdade real ou substancial), onde o juiz deveria

[89] *Idem,* p. 108.

armar-se de absoluta liberdade e de ilimitados poderes na sua atuação com vista a descobrir a verdade dos fatos ocorridos. Sobre isso, explicam os mestres Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães Gomes Filho que

> "(...) a liberdade do juiz penal foi vista como instrumento essencial para a realização da pretensão punitiva do Estado: o juiz penal, diversamente do juiz civil, deveria ser dotado de poderes ilimitados, para efeito do acertamento dos fatos, porque a descoberta da verdade, obtida de qualquer forma, é a premissa indispensável para alcançar o escopo 'defesa social'. E é assim, que a busca da verdade se transmudou num valor mais precioso do que a proteção da liberdade individual."[90]

Contudo, como destaca Grinover, o processo penal moderno sofreu inúmeras transformações, perdendo o vigor na busca da verdade absoluta, não se justificando mais a colheita de qualquer prova a qualquer custo, já que o ordenamento jurídico, inserido em um Estado Democrático de Direito, exige o desenvolvimento do processo dentro de regras morais e do respeito a garantias individuais, ainda que essas prejudiquem a reconstrução fiel e integral dos fatos pretéritos e em investigação.[91]

Dessa forma, o atual Código de Processo Penal, assim como a Constituição, assumem premissas e princípios dos quais se pode dizer que a ideia central do processo penal tem por fim a realização da justiça do caso concreto, por meios processualmente admissíveis e visando assegurar a paz jurídica dos cidadãos. Nesse sentido, o legislador previu um processo penal originalmente acusatório (porém não puro, mas sim um modelo misto), apoiado na busca de equilíbrio e de proporção entre o exercício da ação penal, como prerrogativa e garantia do Estado de Direito, e entre o respeito pelos direitos e garantias do imputado, concebido como limite constitucional da atividade do poder público.[92] Tal afirmação de Jorge de Figueiredo Dias é complementada pelos autores Canotilho e Moreira, quando destacam que o processo penal se mostra como um sistema com fundamento e limite na dignidade e integridade da pessoa humana, assumindo a inegável desigualdade de armas entre o Estado e o arguido e buscando compensá-la juridicamente por meio de atribuições de garantias de defesa a este.[93] É um processo voltado para a tutela dos direitos fundamentais, impondo determinados limites

[90] GRINOVER, Ada Pellegrini, *et al.* As nulidades no processo penal, 2ª ed., São Paulo: Malheiros, 2000, p. 129.
[91] *Ibidem.*
[92] DIAS, Jorge de Figueiredo. "Por onde vai o Processo Penal Português – por estradas ou por veredas?", em *As conferência do Centro de Estudos Judiciários,* Coimbra: Almedina, 2014, p. 54-56.
[93] CANOTILHO, J. J Gomes e MOREIRA, Vital. Constituição da República Portuguesa Anotada, Vol. I, 4.ª ed., Coimbra: Coimbra Editora, 2007, p. 516.

à atividade investigadora, e tendo como barreira inultrapassável (na maioria dos casos) a área nucelar e inviolável da intimidade.[94]

Contudo, é evidente que como forma de exercício do poder público, é impossível a existência de um sistema processual penal eficaz sem qualquer ingerência nos direitos fundamentais dos cidadãos, de forma que o justo equilíbrio se encontra na ponderação adequada dos interesses da prossecução penal do Estado e dos direitos individuais.[95] O Estado não deve ser, por um lado, um Estado-polícia com poderes ilimitados, sob pena de o combate à criminalidade gerar uma verdadeira "criminalidade de Estado"; e, por outro lado, não deve ser também um Estado-observador, que em nada intervém, acabando por valer a "lei do mais forte".[96]

Trata-se, portanto, de uma tentativa de concretização da concordância prática entre as finalidades contraditórias do processo penal de realização da justiça, descoberta da verdade material, proteção dos direitos individuais e restabelecimento da paz jurídica. Dessa forma, o direito processual pode ser definido, nas palavras de João Conde Correia, como um

> "instrumento privilegiado de agressão aos direitos, liberdades e garantias individuais e, ao mesmo tempo, um meio indispensável para a sua protecção. A sua observância é, por isso mesmo, uma garantia fundamental, que confere segurança, previsibilidade e certeza aos cidadãos."[97]

Ou seja, a busca da verdade no processo penal de um Estado de Direito não pode ser realizada a qualquer preço, mas tão somente por meio das vias legitimas. É por isso que faz sentido falar não em verdade "objetiva", mas sim de verdade "forense" ou obtida de acordo com as "formalidades judiciais".[98] Mas, se por um lado o Estado deve abdicar de condenar um criminoso quando a única prova da sua culpa pode ser obtida somente com meios inadmissíveis num Estado de Direito ou desproporcionais ao caso concreto, por outro lado justifica-se que o Estado em certos casos vá mais longe que em

[94] RAMALHO, David Silva, 2017, p. 182-183.
[95] *Idem*, p. 183.
[96] GOSSEL, Karl Heinz. *El Derecho Processal Penal en el estado de Derecho*, Buenos Aires: Rubinzal – Culzoni Editores, 2007, p. 146-147.
[97] CORREIA, João Conde. Contributo para a análise da inexistência e das nulidades processuais, Coimbra: Coimbra Editora, 1999, p. 191.
[98] HASSEMER, Winfried. *Fundamentos del derecho penal*, trad. de Arroyo Zapatero y Muñoz Conde, Barcelona: Bosch, 1984, p. 190.

outros na procura da verdade, avançando gradualmente ao limite, até então intransponível, da dignidade e integridade pessoal do visado.[99]

Portanto, cabe ao Estado analisar e decidir qual o preço (ou seja, o sacrifício de direitos fundamentais e processuais para a prossecução penal de delinquentes) que está disposto a pagar pela busca da verdade. Sacrifício esse que materialmente executado na fase de inquérito condiz, segundo Ramalho, com a utilização de

> "um *arsenal* de meios de investigação criminal progressivamente mais agressivos dos direitos dos cidadãos em função da gravidade e danosidade social do crime em causa ou da absoluta indispensabilidade do meio de prova em face das circunstâncias".[100]

O autor continua, referindo que à medida que esse sacrifício vai aumentando, a investigação criminal passa a atuar sem restrição dos limites pessoais e temporais do concreto processo-crime em que ocorre, atingindo pessoas distintas do visado, que eventualmente são encontradas no caminho da investigação. Sacrifício esse que pode chegar ao ponto de corroer a liberdade de atuação do cidadão comum, que passa a ter constante receio da ocorrência de uma ingerência estatal remota e secreta, preventiva ou repressiva, nas atividades da sua vida.[101]

Nos últimos tempos tais sacrifícios têm sido muito encorajados pelos *discursos de emergência*, que vem influenciando a legislação, a jurisprudência e grande parte da doutrina, que argumenta que em certos casos as investigações chegam a um ponto morto por insuficiência de ferramentas processuais adequadas na legislação processual. Ao utilizar o conceito de *discursos de emergência*, Roxin defende que caberia ao Estado afrontar as novas formas de criminalidade com o uso de *armas* não convencionais, legitimando soluções de exceção contra os chamados "estranhos à comunidade".[102]

Tais discursos de emergência invocam como motivação das reformas processuais tendentes á adotar novas ferramentas mais efetivas para a investigação penal a mudança social produzida pelos lamentáveis sucessos violentos que tem causado grande sensação de insegurança a nível mundial. O terrorismo, o tráfico internacional de entorpecentes e o crime organizado, que perturbam intensamente a paz pública, são vistos como uma ameaça que deve ser acompanhada por um direito penal e processual penal capaz de lutar de maneira efetiva, munida de medidas de investigação

[99] RAMALHO, David Silva, p. 185.
[100] *Idem*, p. 185-186.
[101] *Idem*, p. 186.
[102] ROXIN, Claus. 2008, p. 15-16.

que habilitam a ingerência sem limites em âmbitos de intimidade constitucionalmente protegidos, tendo em vista que tal criminalidade coloca o Estado em uma situação de emergência (uma espécie de estado de necessidade) que legitima a adoção de medidas extraordinárias. Nesses casos, o delinquente se converte tendencialmente em inimigo, e o direito penal, em "direito penal do inimigo".[103]

Esse novo direito penal, proposto inicialmente por Gunter Jakobs e que posteriormente adquiriu seguidores ao longo da doutrina de diversos países, tem uma repercussão direta na esfera privada do visado, onde o "ente despersonalizado" fica despido da sua esfera jurídica, deixando de lhe ser aplicado o Direito Penal do cidadão, passando ele a fazer parte do Direito Penal do Inimigo, havendo um efeito de subtração dos impedimentos legais do Estado na intervenção do círculo privado do inimigo, que se encontra sob total suspeita e vigilância, o que nunca ocorre no Direito Penal do cidadão.[104]

E de fato, seja por influência da doutrina referida acima ou não, está se observando cada vez mais a emersão de novas linhas de equilíbrio entre a segurança e a liberdade (a autonomia, os direitos processuais), com a balança a inclinar-se cada vez mais para o primeiro dos lados. É com base nisso que se trás a pergunta formulada por Muños Conde de forma incômoda, provocativa e claramente agressiva:

> "No sería preferible para aumentar la eficácia del derecho penal en la lucha contra la criminalidade reducir lãs garantias del imputado en el processo penal y permitir valorar las pruebas obtenidas ilegalmente incluso com vulneración de derechos fundamentales, cuando com ellas se consiga obtener la verdad material y la condena del verdadero culpable?"[105].

Contudo, tal manobra se mostraria arriscada e confrontaria os anos de evolução dos direitos fundamentais e do próprio Estado democrático de Direito, sendo admissível apenas nos casos de extrema violência e necessidade, e respeitando sempre o princípio da proporcionalidade, como veremos á frente.

---

[103] *Idem*, p. 18.

[104] Sobre isso, ver: JAKOBS, Gunther e MELIÁ, Manuel Cancio. Direito Penal do Inimigo: noções e críticas, org. e trad. André Luis Callegari, Nereu José Giacomolli, 2ª ed., Porto Alegre: Livraria do Advogado, 2007.

[105] CONDE, Francisco Muñoz. *De nuevo sobre el derecho penal del enemigo*, 2ª ed., Buenos Aires: Hammurabi, 2007, p. 57-66.

## 2. Proibições de prova

Visando resguardar os limites da dignidade humana (art. 1º da CRP) e os princípios do Estado democrático de Direito (art. 2º da CRP), o legislador constitucional prescreveu no artigo 32°, nº 8 da CRP, a nulidade de "todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral de pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações".

No primeiro caso, é absoluta a impossibilidade da utilização da prova obtida com violação do direito á integridade pessoal (art. 25º da CRP), pois se trata de direitos fundamentais cuja compressão é absolutamente intolerável em processo penal, tratando-se aqui de um núcleo irredutível da dignidade humana que pertence também ao criminoso mais brutal, não sendo legítimo que o Estado, ainda que no intuito de perseguir criminosos, pratique ele mesmo crimes.

Já no segundo caso é prevista uma proibição relativa para os casos de intromissão na vida privada, domicílio, correspondência ou telecomunicações, onde o critério para a proibição da prova fundamenta-se no caráter abusivo da intromissão, ocorrendo fora dos casos e termos previstos na lei (como expõe o artigo 34º, nº 2, 3 e 4) ou em violação do principio da proporcionalidade nos seus diversos aspectos (conforme art. 18º da CRP).

Em 1987 tais regras constitucionais foram materializadas no artigo 126º do CPP, sob o título de *métodos proibidos de prova*, onde no nº 1 e 2 foram reiteradas as mencionadas proibições absolutas; e no nº 3 foi prevista a admissibilidade das provas obtidas com intromissão na privacidade do visado quando executada pela autoridade competente e nos estritos termos da lei, ou quando o titular dos direitos afetados esteja de acordo com a intromissão.[106]

Os efeitos das proibições de prova recaem também nos meios de prova obtidos direta ou indiretamente a partir do meio de prova proibido, tratando-se de um limite auto-imposto pelo Estado na descoberta da verdade, onde a sua violação, seja pela

[106] Nesse mesmo sentido, cita-se o nº 2, do art. 8º da Convenção Europeia dos Direitos do Homem: *"Não poderá haver ingerência da autoridade pública no exercício do direito [à vida privada e às comunicações] salvo se esta ingerência estiver prevista em lei e constitua medida que, em uma sociedade democrática, seja necessária para a segurança nacional, a segurança pública, o bem-estar econômico do país, a defesa da ordem e a prevenção de infrações penais, a proteção da saúde ou da moral, dos direitos e das liberdades dos demais."*

prática de um ilícito penal ou quando atentatória da dignidade humana, atinge a própria legitimidade do exercício do poder punitivo do Estado.[107]

É nesse sentido que Muños Conde entende que a busca da verdade no processo penal é uma das tarefas mais apaixonantes, complexas e difíceis de resolver pelos tribunais de justiça, mas nenhuma dessas dificuldades se compara com a limitação imposta pelas próprias normas jurídicas que obrigam (pelo menos nos Estados de Direito) a levar em conta e a respeitar nesta tarefa determinados princípios e direitos fundamentais do acusado, que impedem a valoração de provas obtidas ilicitamente ou com violação de direitos fundamentais, como, por exemplo, através da tortura, ou da utilização ilícita de meios audiovisuais, por mais que estes podem conceder um grau de certeza quase total sobre a verdade do feito que se está julgando.[108]

Importante referir que o conceito de proibições de prova, conforme por Ramalho, engloba tanto as proibições de produção de prova como as proibições de valoração de prova. O primeiro caso pode ser dividido em três tipos: as proibições de temas de prova, que demandam que certos fatos não podem ser investigados; as proibições de meios de prova, que proíbem a utilização de certos meios de prova independentemente da sua potencial utilidade para a descoberta da verdade; e os métodos de prova absoluta ou relativamente proibidos, que se tratam do banimento da utilização de certos procedimentos para a obtenção de meios de prova e respectiva utilização. Já o segundo caso trata-se da proibição de utilização de certos meios de prova como fundamento da prolação de decisões desfavoráveis ao arguido, de modo que a proibição de valoração de prova poderá decorrer da verificação de uma proibição de produção de prova, ou poderá ser independente.[109]

As proibições de valoração de prova independentes, para David Silva Ramalho,

> "ao não pressuporem a verificação de qualquer vício na produção da prova, afectarão meios de prova obtidos com recurso a métodos lícitos, vedando a sua valoração (i) por força de disposição legal (por exemplo, os conhecimentos fortuitos no âmbito de uma escuta telefônica que não preenchem os requisitos do artigo 187º, nº 7, do CPP) ou (ii) por se afigurar desnecessária, desproporcional ou susceptível de suprimir direitos afectados de tal modo que é legítimo concluir que o interesse da prossecução penal deve passar para segundo plano em relação ao impacto da sua valoração sobre os direitos fundamentais afectados".[110]

[107] MATA-MOUROS, Maria de Fátima, 2011, p. 330-331.
[108] CONDE, Francisco Munõz. Palavras previas a terceira edição de "*La búsqueda de la verdade en el processo penal",* Buenos Aires: Hammurabi, 2007, p. 13-14.
[109] RAMALHO, David Silva, 2017, p. 190-191.
[110] *Idem*, p. 191.

A questão das proibições de valoração de prova sem suporte legal tem se mostrado de difícil resolução, estando de um lado do conflito o interesse público da realização da justiça e do outro lado o interesse público da tutela de direitos fundamentais. Essa problemática é muito bem exposta pelos casos da valoração em processo penal de diários íntimos do arguido contendo manifestações do domínio absolutamente interno do seu autor, sem a sua autorização.

O Tribunal Federal de Justiça da Alemanha (BGH) se manifestou sobre o tema em duas ocasiões distintas.[111] No primeiro caso, em 1964, o diário íntimo foi entregue às autoridades pela esposa do amante da autora do diário, onde o seu conteúdo tratava, entre outras coisas, sobre a relação amorosa entre ambos, a qual foi negada em julgamento pela autora. Ao manifestar-se sobre a possível prática de um crime de falso testemunho em razão do caráter contraditório das declarações prestadas em julgamento e das escritas no diário íntimo, o Tribunal entendeu que se o diário (que é da esfera de personalidade do autor e se este não quer que o seu conteúdo seja de conhecimento de terceiros) for trazido, contra sua vontade, para servir de prova em processo penal, existe um atentado á dignidade humana e ao direito fundamental de livre desenvolvimento da personalidade, a menos que o interesse do Estado na punição do crime, pesado á luz dos direitos fundamentais, seja mais relevante do que o interesse pessoal na proteção do seu próprio domínio de segredo.[112]

Já no segundo caso (1987), o Tribunal entendeu pela admissibilidade da valoração do diário. Estava em causa um homicídio onde houve um ataque de machado nas costas da vítima, e o diário, que foi escrito por recomendação médica em razão da terapia praticada pelo acusado, continha referência á incapacidade do autor em lidar com mulheres e á sua inclinação para realizar atos sexuais violentos. Nesse caso, o mesmo Tribunal veio a confirmar a decisão recorrida concluindo que a tutela da intimidade, e, de uma maneira geral, do direito de personalidade, não podem valer ilimitadamente, tendo em conta a necessidade de uma justiça funcionalmente capaz, bem como atendendo á gravidade do crime em causa, devendo ser admitida a valoração do diário.[113]

Concordando com o entendimento do Tribunal, Santos Cabral sustenta que

[111] Informações sobre os casos podem ser encontras na fundamentação do acórdão do TC, de 5/12/2003, Proc. 593/03, Relator: Benjamim Rodrigues, disponível em www.tribunalconstitucional.pt
[112] RAMALHO, David Silva, 2017, p. 192.
[113] *Idem*, p. 193.

> "a confissão que o homicida em série produz no seu diário sobre os crimes que praticou, não é mero diálogo no interior da sua circunstância mais íntima ou uma confissão consigo próprio, mas uma afirmação da sua forma de aniquilar o Outro e a sua concretização no mundo exterior dos seus impulsos primitivos. Tal confissão, não é uma questão pessoal centrada na reflexão mais íntima, mas um assunto de Comunidade que tem um direito legítimo de se defender"[114].

Posteriormente, em 1989, o BVerfG (Tribunal Constitucional Federal) veio a ser chamado no segundo caso do diário para manifestar-se sobre a constitucionalidade da sua valoração em processo penal. O Tribunal começou a fundamentar sua decisão com base na jurisprudência que segue sobre a teoria do núcleo, reconhecendo unanimemente a existência de "um domínio último intocável de conformação da vida privada que é, sem mais, retirado ao poder público", considerando que "mesmo os interesses mais importantes da comunidade não podem justificar atuações nesse campo; uma ponderação segundo o princípio da proporcionalidade não tem aqui lugar". Entretanto, o Tribunal referiu que o mero registro de informações em diário não é excluído automaticamente do âmbito de atuação do Estado, de modo que primeiramente é necessário analisar o caráter e significado do seu conteúdo para então verificar sua possibilidade de utilização no processo penal. Dessa forma, o Tribunal entende que se as informações constantes no diário reportam o planejamento de ilícitos criminais ou a descrição de crimes já cometidos, a sua imediata conexão com ações concretas e puníveis criminalmente excluía-as do domínio intocável da vida privada, não havendo vedação constitucional da sua utilização e valoração.[115]

A ponderação dos interesses em confronto (os direitos fundamentais do arguido de um lado e a descoberta da verdade em processo penal do outro) deverá ir para além da análise, em abstrato, da admissibilidade da sua utilização, mas também para uma análise do caso concreto em que se verificará se a utilização das informações do diário se revelam necessárias e adequadas para a investigação do crime e se a intervenção na esfera privada do arquido não é desproporcional em relação ao objetivo de descoberta da verdade no processo penal. Dessa maneira, da análise do caso em questão, Ramalho ressalta que quatro juízes votaram no sentido da admissibilidade da valoração das

[114] CABRAL, José Santos. "Anotação ao artigo 126º - Métodos proibidos de prova", Código de Processo penal comentando, Coimbra: Almedina, 2014, p. 443. Em sentido contrário, criticando tal entendimento, ver: ROXIN, Claus. *La evolución de la Política criminal, el Derecho penal y el Processo penal*, Valencia: Tirantlo Blanch, 2000, p. 151.
[115] RAMALHO, David Silva, 2017, p. 194.

informações do diário, afirmando que o mesmo não pertencia à área nuclear da intimidade imune ao poder público, tendo em vista que o acusado transcrevera as suas idéias em papel, excluindo-as assim do seu âmbito interno, de modo que a sua transcendência afeta a coletividade permanentemente. Já os outros quatro juízes concluíram que o diário apresentava natureza de monólogo íntimo, pertencente à área nuclear da intimidade do indivíduo, motivo pelo qual deve ser excluído de qualquer ingerência estatal.[116]

Importante referir que o Tribunal Constitucional Federal alemão, a partir do caso exposto, desenvolveu uma teoria chamada da teoria dos três níveis, explicada por Jaeger da seguinte forma: 1) o primeiro nível está constituído especialmente pelas notas e apontamentos íntimos que pertencem ao âmbito nuclear dos direitos de personalidade, que são absolutamente inutilizáveis sem a possibilidade de uma ponderação de interesses; 2) o segundo nível se refere ás declarações menos intimas que estão classificadas dentro da esfera meramente privada (a qual, no caso concreto, pode facilmente ser confundida com a esfera intima em razão das suas estreitas fronteiras). Aqui há de se decidir a questão do emprego da prova partindo de uma ponderação entre os interesses privados e os interesses da persecução penal; 3) já o terceiro nível constitui o âmbito dos contatos sociais de ordem geral, os quais não requerem uma proteção excepcional, como por exemplo o diário de procedimentos comerciais. Aqui se pode utilizar o conteúdo do diário sem qualquer ponderação.[117]

Nessa linha, as soluções encontradas pela jurisprudência do Tribunal Constitucional alemão (se assemelhando com a jurisprudência Portuguesa) para a problemática das proibições de valoração de prova independentes, levaram em conta uma ponderação dos interesses concretamente em confronto e a existência de um núcleo intangível da intimidade pessoal que atua como um limite absoluto daquela ponderação. Ainda, quanto maior a ingerência estatal, maior será a proteção da esfera privada do visado, ingerência essa que além de dever ser prevista legalmente pelo legislador, deverá aduzir uma ponderação casuística da necessidade, adequação e proporcionalidade da mesma em face dos valores em conflito, a ser realizada pelo aplicador do Direito.[118]

---

[116] *Idem*, p. 194-195.
[117] JAGER, Christian. *Problemas fundamentales de derecho penal y procesal penal*, Buenos Aires: Fabian J. Di Placido, 2003, p. 93-94.
[118] RAMALHO, David Silva, 2017, p. 197-198.

Ou seja, como acrescenta João Conde Correria, não basta que a lei permita a apreensão de um diário íntimo, é necessário também que após a ponderação dos interesses em jogo, se verifique que a valoração das informações do diário seja justificada em razão da importância desse elemento probatório para prova de um crime onde a gravidade, natureza, modo de execução e valores jurídicos violados permitam fazer prevalecer o interesse coletivo de uma perseguição penal eficaz sob o interesse individual do arguido.[119]

Portanto, no que se refere a ponderação de valores e a intransponibilidade da área nuclear da intimidade, a jurisprudência do Supremo Tribunal de Justiça entende que o direito á intimidade da vida privada não é um valor absoluto, devendo ceder diante de interesses fundamentais como a eficiência da justiça criminal no combate á criminalidade grave, de modo que a "teoria das esfera e núcleo intocável" deve ser relativa até certo ponto, mas absoluto quando atinge o insuperável núcleo da dignidade do Homem. A grande questão é saber onde começa e onde termina tal núcleo essencial de forma a não gerar uma margem de insegurança e vacuidade.[120]

Mas ao analisar se deve existir ou não uma área *blindada* á intromissão estatal, onde independe dos interesses e valores em causa e da necessidade daquele meio de prova, o Supremo Tribunal de Justiça entende que "o respeito pela dignidade e intimidade de cada cidadão acaba quando o mesmo desrespeita a dignidade dos outros cidadãos e os valores fundamentais prosseguidos pelo Estado como é o caso da funcionalidade da justiça penal", concluindo que é portanto, é possível afirmar que a decisão do Tribunal foi acertada, respeitando o princípio da proporcionalidade, tendo em vista que apenas a extrema necessidade e particularidades do caso em questão é que levaram a superação da área *blindada.*

> "incontornável o pressuposto de que dificilmente se pode afirmar um núcleo inviolável de dignidade a respeitar quando o que está em causa é a perseguição penal do agente que coloca em causa direitos fundamentais como é a vida dos seus concidadãos (por exemplo, a leitura do diário intimo do *serial killer* revelando a sua psicopatia, ou a situação da desresponsabilização do injustamente condenado)".[121]

[119] CORRERIA, João Conde. "Questões práticas relativas á utilização de diários íntimos como meio de prova em processo penal", em Revista do CEJ, nº 6 (1º semestre de 2007), p. 139-141.
[120] Conforme Acórdão do STJ, de 03.03.2010, Proc. 886/07.8PSLSB.L1.S1, Relator Santos Cabral.
[121] *Idem.*

Portanto, é possível afirmar que a decisão do Tribunal foi acertada, respeitando o princípio da proporcionalidade, tendo em vista que apenas a extrema necessidade e particularidades do caso em questão é que levaram a superação da área *blindada*.

# III. OS DIREITOS FUNDAMENTAIS, O PROGRESSO TÉCNICO-CIENTÍFICO E OS MÉTODOS OCULTOS

As aceleradas transformações técnico-cientificas das últimas décadas atingem diretamente o direito e, particularmente, o direito processual-penal, que passa a contar com um arsenal de novos métodos de investigação e intromissões na vida privada, legitimadas pela prossecução das finalidades da investigação criminal. Ocorre que a evolução das tecnologias, e consequentemente das novas formas de investigação, acontecem de uma maneira tão acelerada que o legislador se vê em uma difícil missão de acompanha-las, e como consequência disso acaba criando (ou não criando) leis incapazes de resguardar os diversos direitos fundamentais em jogo. Nessa linha, Costa Andrade entende que

> "de um lado, a progressão – expressa na emergência e triunfo de novos direitos fundamentais ou de novas dimensões dos direitos preexistentes – é espontânea, contínua e automática, apenas dependendo da consciência jurídica, ás mãos da doutrina e da jurisprudência (constitucionais). Diferentemente, do outro lado, o caminho – *sc.* a consagração de novos meios de obtenção de provas resultantes do aproveitamento das possibilidades de intervenção e intromissão oferecidas pelas realizações técnico-científicas – faz-se de forma descontinua e derivada, ao ritmo das sucessivas e localizadas intervenções do legislador"[122].

É nesse sentido que é possível afirmar que a evolução técnico-cientifica para o processo penal se mostra simultaneamente como heroína e vilã, onde de um lado alarga as possibilidades de investigação do crime, aumentando as probabilidades de sucesso do Estado na perseguição de criminosos, e do outro invade e atinge todo um conjunto de valores e direitos, em geral relacionadas à integridade, dignidade e autonomia pessoais, ás esferas do segrede e reserva, entre outros. Em razão disso que no espaço de poucas décadas se viu a emergência e triunfo de direitos como a *palavra*, a *imagem*, a *autodeterminação informacional*, e a mais recente, a *integridade e confidencialidade dos sistemas informáticos*. Avanços esses que não dependem da intervenção do legislador, sendo fruto da doutrina e jurisprudência, cabendo tão somente dar nome e dimensões á direitos já consagrados e estabilizados. Mas como referido, ao contrário dos direitos fundamentais, a legitimação dos novos meios de investigação possibilitados pelo avanço tecnológico depende de expressa e inequívoca intervenção do legislador,

[122] ANDRADE, Manuel da Costa, 2009, p. 148.

pois se o surgimento e alargamento dos direitos fundamentais não dependem de prévia e necessária intervenção legislativa, a sua limitação e compressão sim.[123]

Nessa linha, trataremos da relação entre o progresso técnico-cientifico, os meios ocultos de investigação e alguns dos direitos fundamentais mais atingidos pelos mesmos, socorrendo-se, sempre que possível, das lições da jurisprudência alemã e americana, que muito já desenvolveram sobre o tema.

## 1. O direito fundamental à reserva da intimidade da vida privada

Em nível internacional este direito vem consagrado no artigo 12.º da Declaração Universal dos Direitos do Homem, no artigo 8.º da Convenção Européia dos Direitos do Homem, bem como no artigo 17.º do Pacto Internacional de Direitos Políticos e Civis. No ordenamento jurídico português, este direito é tutelado a nível constitucional, no artigo 26.º n.º 1 da CRP. Alguns outros direitos fundamentais funcionam como garantia deste, nomeadamente o direito à inviolabilidade do domicílio e da correspondência (artigo 34.º) e da proibição de tratamento informático de dados referentes à vida privada (artigo 35.º n.º 3).

A Constituição incumbe à lei de estabelecer garantias efetivas para a proteção do direito á reserva da intimidade da vida privada. Porém, se mostra como uma árdua tarefa delimitar o âmbito de proteção da norma, nomeadamente saber aquilo que concretamente se deve entender por vida privada e quais os seus limites ou a sua extensão.

Assim, para que seja possível entender o significado do direito à privacidade na atualidade, se faz imprescindível percorrer alguns importantes momentos históricos, tendo em vista que o direito de privacidade experimentou profundas modificações ao longo do tempo. Todavia, o que não se pode dizer que sofreu modificações ao longo da evolução humana, é a necessidade que o indivíduo possui de preservar alguns fatos e acontecimentos do conhecimento público e do Estado.

Para algumas sociedades antigas, a ideia de privacidade foi inadvertidamente confundida com o exercício do próprio direito de propriedade, onde somente os indivíduos possuidores de propriedades poderiam praticar atos sem a observância do público, servindo a propriedade como um escudo protetor em face das ingerências

[123] *Ibidem.*

alheias. Esse instituto fora por bastante tempo fundamentando e justificado, em Roma, na reserva das práticas religiosas, da qual a participação era restrita aos membros familiares. Mas mesmo com tais manifestações de respeito e atenção à vida privada e aos atos que contornavam a esfera íntima dos indivíduos na antiguidade, a privacidade ainda não era possível de ser reconhecida como direito autônomo, conforme defendido por Sylsvestre e Lima.[124]

Para o escritor espanhol Perez Luño, o surgimento do conceito de privacidade estaria estritamente relacionado ao nascimento da burguesia, tendo em vista que a intimidade era configurada como uma aspiração pelos burgueses para ascender ao que antes havia sido privilégio de poucos. Aspiração essa que foi potencializada pelas novas condições de vida, pois assim como no período medieval, onde o isolamento era privilégio das mais altas esferas da nobreza, ou daqueles que por vontade própria renunciavam a vivencia comunitária, a burguesia aspirava tais privilégios sob o pretexto da privacidade.[125]

Posteriormente, sob influência do pensamento liberalista, a intimidade da vida privada passou a ser justificada na ideia de que os únicos aspectos da vida humana que causariam deveres e responsabilidades eram aqueles que afetavam outros indivíduos. Assim sendo, os aspectos que dizem respeito apenas à vida do indivíduo seriam de plena e exclusiva gerência deste, como suas ideologias, suas escolhas, pensamentos e sentimentos. Nesse contexto, a privacidade ganhou fortes traços liberais, o que acabou por proporcionar uma maior fortificação da sua essência e estrutura, apesar de ainda não gozar de reconhecimento e autonomia.[126]

Foi apenas em 1890, nos Estados Unidos, que Samuel Warren e Louis Brandeis publicaram na Harvard Law Review um artigo intitulado "The Right to Privacy[127]", onde defenderam a autonomização da proteção e refrações da personalidade humana, considerando não mais poderem ser protegidas pela invocação da violação de um direito de propriedade privada, da confiança, da honra, ou de qualquer obrigação de tipo contratual.

---

[124] SYLSVESTRE, Fabio Zech e LIMA, Pedro Souza. O direito fundamental á privacidade em face da administração pública, 2012. Disponível em: http://editora.unoesc.edu.br/index.php/simposiointernacionaldedireito/article/view/1586/1041. Acesso em: 17/02/2018.

[125] PÉREZ-LUNO, Enrique. *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 2005.

[126] *Ibidem.*

[127] WARREN, Samuel D. e BRANDEIS, Louis D. *The Right to Privacy*, Harvard Law Review, Vol. 4, Nº 5, 1898. Disponível em: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

Assim, passou a defender-se a tese de que o *common law* teria evoluído da proteção da personalidade física para a tutela dos pensamentos, emoções e sensações do indivíduo, dando lugar à consolidação de um princípio autônomo denominado de direito à privacidade, sendo que sua violação resultaria em responsabilidade por ato ilícito e a consequente fixação de indenização por perdas e danos. Tal concepção desenvolvida pelos professores americanos do século XIX condiz a uma dimensão humana merecedora de proteção face aos perigos provocados pela massificação da difusão de informações através da imprensa escrita, também identificada pelo "Right to be let alone", ou seja, o direito de estar só (tese esta que irradiou do pensamento jurídico norte-americano para os demais sistemas jurídicos).[128]

Portanto, constata-se que a dimensão do conteúdo do direito à privacidade parte de um instrumento hábil para defesa da propriedade, em uma concepção burguesa, e evolui até o reconhecimento de um direito próprio e autônomo, voltado a proteger os pensamentos, as emoções e sensações dos indivíduos, ou seja, aspectos ligados à vida privada e a intimidade do ser humano.

Contudo, na "sociedade da informação", ou da "Era Digital", em que vivemos nos dias atuais, onde existem diversos elementos capazes de ameaçar os direitos fundamentais referentes à vida privada, a noção do *right to privacy*, delineado no final do século XIX, já não mais responde aos anseios do conteúdo do direito à privacidade. Ademais, na sociedade atual, os cidadãos presenciam o fenômeno *massmedia*, onde os meios de comunicação são ferozmente ciosos ao destino do cidadão, visando satisfazer à insaciável "máquina de sensações" desejada pelo público, tornando a informação, mesmo que desinteressante, uma forma de obtenção e manutenção de poder.

A elaboração de um conceito atual do direito de privacidade trata-se de uma tarefa complexa devido ao grau de abstração que envolve o mesmo, inclusive pelo fato de existir uma linha muito tênue entre a demarcação do campo da vida privada que goza da reserva de intimidade e o campo "aberto" à publicidade.

Para Miller[129], a privacidade é difícil de ser definida porque é expressamente vaga e imperceptível. As numerosas definições legais, assim como o conjunto de decisões jurisprudenciais que tutelam este direito, não contêm uma definição precisa do conteúdo do direito à privacidade. E mais, na maior parte das situações, não tentam estabelecer nenhum conceito, limitando-se a tipificar, com maior ou menor

[128] *Ibidem.*
[129] MILLER, Arthur R. *The Assault on Privacy*, Michigan: University of Michigan Press, 1970, p. 259.

flexibilidade, os supostos atentados ou a estabelecer a existência das condutas que a ameaçam.

Ainda, devemos considerar que a privacidade possui um certo caráter subjetivo, de modo que uma pessoa pode ter a intenção de que determinado fato não se torne público, pois considera-o íntimo e pessoal; já outra pessoa, que tenha se envolvido no mesmo fato ou compartilhado a mesma ideia, pode não ter a mesma percepção, não se preocupando com a divulgação e publicidade de tais informações.

Portanto, o intérprete, para chegar ao âmbito de proteção do direito à privacidade do indivíduo, talvez deva partir da própria noção de privacidade prevista na carta constitucional associada com a ideia da dignidade da pessoa humana, de modo a definir-se a amplitude da esfera privada de cada pessoa, culturalmente ajustado à vida contemporânea. Ou seja, como explicado por Jorge de Figueiredo Dias, será sempre um conceito de conteúdo variável, na medida em que a sua extensão e o seu grau e âmbito de proteção serão sempre mutáveis, resultando em um conceito cultural, que varia com o tempo, o espaço, e o tipo de pessoas em causa.[130]

Entre os contributos doutrinários na tentativa de delimitação do conteúdo do direito em tela, a doutrina italiana, tendo como expositor Frosini[131], explica a privacidade como sendo uma espécie de retiro voluntário e temporal de uma pessoa que se isola da sociedade, por meios físicos ou psicológicos, para buscar a solidão ou estabelecer uma situação de anonimato ou de reserva.

Já o autor Solove[132] desenvolveu um estudo que contribuiu significativamente para a devida compreensão do conceito atual do direito à privacidade, entendendo que o conteúdo jurídico deste direito engloba as seguintes perspectivas: a) a liberdade ou segurança frente a qualquer tipo de intromissão indevida na esfera privada (*freedomfromunreasonableserch/limitedaccestothe self*); b) o direito do indivíduo de guardar ou compartilhar fatos que não deseja que ganhe notoriedade (*secrecy*); c) a garantia do respeito às opções pessoais em matéria de associação ou crenças (*privacyofassociationandbelief*); d) a tutela da liberdade de escolhas sem interferências alheias (*privacyandautonomy/personhood*); e) possibilidade dos indivíduos e grupos de

[130] DIAS, Jorge de Figueiredo. "*Direito à informação, protecção da intimidade e autoridades administrativas independentes*", Estudos em Homenagem ao Professor Doutor Sérgio Soares, Coimbra: Coimbra Editora, 2001, p. 627.
[131] FROSINI, Vittorio. *Informática y Derecho*, Bogotá: Editorial Temis, 1988, p. 107.
[132] SOLOVE, Daniel J. *Conceptualizing Privacy*. California: California Law Review, 2002, p. 1092. Disponível:http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.

ter e controlar as informações que lhes dizem respeito, ou seja, controle de informações pessoais (*informationcontrol/ control over personalinformation*) e f) a intimidade (*intimacy*).

Portanto, como se pode observar, a privacidade pode ser concebida como o poder de exercer um controle sobre as informações que podem afetar a cada pessoa individual ou coletivamente, tendo como conteúdo, dentre outros elementos, a liberdade de pensamento, controle do próprio corpo, controle sobre informações pessoais (como sentimentos e ideias), da proteção da reputação e o direito de estar reservado longe das observações de outras pessoas, inclusive do Estado. Ainda, independentemente da teoria adotada, a sua definição parte sempre de uma distinção entre uma área nuclear da privacidade "absolutamente" inviolável e uma outra área, ainda que privada, já susceptível de ser restringida, com observação dos limites decorrentes da dignidade da pessoa humana e do respeito pelas exigências do princípio da proporcionalidade.

Contudo, como já referido, nos últimos tempos são incontáveis as ameaças que a privacidade corre, tendo em vista o avanço tecnológico e as novas formas de investigação e vigilância nas mãos do Estado (e de terceiros mal intencionados). Segundo Andrade, para o processo penal, o sacrifício da privacidade estará legitimado sempre que necessário e adequado á salvaguarda de interesses ou valores superiores, respeitadas as exigências do princípio da proporcionalidade. Todavia, se não usadas de maneira coerente e legítima, as novas formas de obtenção de prova demonstram um alto potencial de lesividade para a privacidade do visado, das pessoas ao seu redor, e, de um modo geral, para toda sociedade.[133]

A ameaça que tecnologias e computadores são para o resguardo da privacidade era algo previsto há muito tempo. Em 1890, Louis Brandeis e Samuel Warren, no já mencionado artigo "The Right to Privacy", advertiram que dispositivos mecânicos ameaçavam de que o que fosse sussurrado dentro de casa poderia ser ouvido de fora. Após, em 1970, Arthur Miller advertiu que uma "Sociedade de Dossiês" alimentada por computadores ameaçaria destruir a essência dessa privacidade pessoal que é fundamental para a democracia. Os oitenta anos entre estas duas advertências foram preenchidos com invenções e técnicas comercias sofisticadas tornando cada vez mais impossível para assegurar a cada individuo o seu direito de ser "deixado sozinho". Miller também previu em seu livro o perigo de vivermos em uma sociedade muito

[133] ANDRADE, Manuel da Costa. Sobre as Proibições de Prova em Processo Penal¸ Coimbra: Coimbra Editora, 1992, p. 95.

ocupada ou ingênua para reconhecer os sintomas da sufocação do computador, que se mostra incomparável como um repositório de conhecimento e dispositivo de solução de problemas, mas como a maioria dos outros significativos avanços industriais, há um tremendo *feed-back*, que é o sacrifício da privacidade[134] (algo parecido já havia sido exposto por George Orwell em seu livro "1984", quando criou a figura do "*Big Brother*").

E cada vez mais isso se torna uma realidade. Seja com a utilização constante da Internet e, em especial, dos *smartphones* e das redes sociais (como por exemplo, o *Facebook, Instagram, Twitter*), através das quais é possível saber (quase) tudo acerca da vida pessoal dos usuários; seja pela quantidade de informações pessoais que as pessoas armazenam em dispositivos eletrônicos, estando à mercê de uma ingerência estatal ou de terceiros, podendo obter o mais variado tipo de informações (como é o caso do diário pessoal tratado anteriormente), ou seja em razão das bases de dados pessoais criadas pelas empresas e pelo Estado, informatizando praticamente todos os aspectos da vida.

Quando alguém navega na Internet, participa de fóruns e redes sociais, realiza operações de comércio eletrônico, e faz *download* de arquivos e documentos, está revelando dados acerca da sua personalidade, de modo que separadamente podem não significar muito, mas se analisados em conjunto tais dados representam uma ameaça para o núcleo mais profundo da intimidade.

Sobre isso, importante trazer o *direito á autodeterminação informativa*, sendo definido como o direito que os cidadãos têm de conhecer quem, quando e em que circunstâncias são sabidas informações sobre eles, sendo uma verdadeira proteção dos indivíduos frente á um ilimitado emprego, arquivo e retransmissão dos seus dados pessoais. O protetor constitucional germânico, já em 1969, se manifestou sobre a afetação dos direitos fundamentais devido as condições "atuais" e futuras do processamento automático de dados, referindo que seria incompatível com a dignidade humana que o Estado pudesse apelar ao direito de registrar e catalogar em forma coercitiva a totalidade da personalidade dos seres humanos, ainda mais anonimamente, tratando-os como uma coisa, pois os indivíduos devem conservar um "espaço interior" ao qual podem se "retirar", podendo permanecer em paz e gozar do seu direito á solidão para desenvolver sua personalidade livre e responsável.[135]

---

[134] MILLER, Arthur R. 1970, p. 259.

[135] Sentença da Primeira Sala do Tribunal Constitucional Alemão, de 16 de julho de 1969 (BvR 19/63) sobre a Lei sobre a Realização de uma estatística da população e da vida economicamente ativa

Conforme lembra Pradillo, recentemente o Tribunal Constitucional alemão voltou a se manifestar sobre a matéria, advertindo sobre a necessidade de se estar atento ao rápido desenvolvimento das tecnologias de informação e do seu uso como medida de investigação, podendo vulnerar o direito constitucional da autodeterminação informativa, no sentido de possibilitar uma vigilância total sobre um sujeito e construir um perfil integral da sua personalidade, o que seria constitucionalmente inadmissível.[136]

E de fato, a ameaça que o desenvolvimento tecnológico representa para a privacidade pessoal e para outros direitos fundamentais parece ser agravada quando observamos o uso das novas tecnologias por parte de instituições governamentais e pela polícia, para investigações criminais e para a manutenção da segurança pública, passando a existir uma verdadeira vigilância dos cidadãos.

Nesse contexto, se mostra interessante a posição tomada pela Suprema Corte dos EUA em relação à Quarta Emenda (proteção da intimidade contra pesquisas e registros). Após muitos casos envolvendo a intimidade e privacidade, a Suprema Corte passou a centralizar a problemática em três elementos principais com a finalidade de responder a pergunta de se um agente estatal superou os limites da Quarta Emenda nos casos em que se empregam "novas tecnológicas" na investigação criminal. Tais elementos são explicados por Jacoby[137] como, primeiro: "qual é o objetivo da vigilância através dos instrumentos tecnológicos?" Pois é evidente que o domicílio de uma pessoa recebe uma maior proteção do que uma propriedade comercial, já que o domicílio é elegido por excelência pelas pessoas para desenvolver sua vida privada. Segundo: "que tipo de informação se revelará com esse tipo de vigilância?" Pois quando a vigilância técnica revela detalhes íntimos e privados é mais provável que se considere que algum dos direitos de privacidade da Quarta Emenda restem vulnerados, já que gravar os movimentos de uma pessoa nas ruas de uma cidade não é o mesmo que no interior de um ginásio, por exemplo. E terceiro e mais importante: "qual é a natureza dos meios técnicos utilizados?". A Suprema Corte dos EUA estimou que a utilização de instrumentos tecnológicos de investigação que são amplamente utilizados e conhecidos pelos cidadãos conduzem a uma menor expectativa de privacidade do que os que são

(microsenso) de 16 de março de 1957 (BGBI I, p. 213), na versão da Lei de 5 de dezembro de 1960 (BGBI I, p. 873).

[136] PRADILLO, Juan Carlos Ortiz. "*El impacto de la tecnología en la investigación penal y en los derechos fundamentales",* em VV.AA. *Problemas actuales de la justicia penal*, Madrid: Ed. Colex, 2013, p. 327.

[137] JACOBY, Nicole. "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality Of Technical Surveillance Measures in Germany and the United States", em *Georgia Journal of Intemational and Comparative Law,* vol. 35, n° 3, 2007, p. 453.

menos conhecidos ou que não estão, em geral, à disposição do público. Ou seja, a Suprema Corte levou em conta a natureza e grau de desenvolvimento da tecnologia aplicada na investigação para determinar se a expectativa razoável do indivíduo à privacidade foi violada ou não, exigindo assim uma ordem judicial previa para habilitar certas atuações da polícia investigadora.

Pradillo contribui com Jacoby citando o exemplo do caso *California vs. Ciraolo* (1986), onde se chegou a conclusão de que a utilização de um helicóptero e uma câmera fotográfica de 35mm para fotografar uma plantação de maconha em uma fazenda não constituía uma violação da Quarta Emenda, já que a droga podia ser simplesmente avistada e o uso de helicópteros e aviões se converteu em uma prática cotidiana a nível comercial, e que a proteção da Quarta Emenda nunca foi ampliada para exigir que a polícia feche seus olhos ao caminhar pela rua, ou, como no caso examinado, ao sobrevoar uma casa, pois a vigilância por helicóptero foi feita de forma visual, sem o emprego de complexos instrumentos tecnológicos. De maneira contrária, no caso *Kyllo vs. United States* (2001), o debate girou em torno de uma investigação onde se utilizaram dispositivos de visão térmica para verificar a partir da via pública emanações térmicas produzidas dentro de um domicilio onde se suspeitava que estivesse sendo cultivada maconha com lâmpadas de raios UVA. O Tribunal sentenciou que a informação revelada por tais dispositivos não seria possível sem a intrusão física em uma zona protegida pela Constituição e que a mesma havia sido obtida com o emprego de tecnologias que não são do uso geral do público, concluindo que havia se realizado uma busca (search) não possível sem uma ordem judicial previa (warrant).[138]

Outra lição importante que pode ser retirada da jurisprudência americana, envolvendo especificamente a privacidade e a obtenção de prova em ambiente digital, é a de que vários tribunais inferiores têm entendido que uma pessoa que instala em seu computador um programa P2P (*peer-to-peer*) que habilita o compartilhamento de arquivos, dando assim a qualquer pessoa com acesso a Internet a possibilidade de acessar o seu equipamento para fazer o *download* de tais arquivos, não pode ter nenhuma expectativa razoável de privacidade com o conteúdo compartilhado do seu computador, de modo que não atinge a Quarta Emenda a possibilidade da policia poder

[138] PRADILLO, Juan Carlos Ortiz. "*El impacto de la tecnología en la investigación penal y en los derechos fundamentales"*. 2013, p. 324.

utilizar um determinado *software* para localizar e descarregar de forma remota tais arquivos, inclusive se o computador visado se encontre no domicilio do suspeito.[139]

De fato, as lições da jurisprudência americana se mostram pertinentes ao ponto que consideram a tecnologia aplicada no caso concreto para analisar se houve/haverá violação da privacidade do visado e se há necessidade de um mandado judicial, tendo em vista que todos os dias as tecnológicas de vigilância e obtenção de prova estão avançando, tornando muito difícil ao legislador acompanhar essa evolução constante com a criação de leis para prever todos os métodos possíveis de obtenção de prova (por mais que seja sabido que o governo americano tem ao seu dispor diversas ferramentas para vigilância de um número indeterminado de pessoas e que frequentemente faz uso das mesmas sem um mandado judicial, como demonstrado para o mundo no caso *Snowden*).

Contudo, tal sistemática pode ser aplicável e eficaz em países onde rege a *common law*, que baseia-se em decisões dos tribunais e não em atos legislativos e executivos, como a *civil law*. De modo que para nós, não basta contentar-se com decisões jurisprudências, sendo imprescindível a intervenção legislativa e exaustiva como resposta do emprego de instrumentos tecnológicos em investigações criminais ocultas, onde há possível afetação desproporcional á intimidade e a outros direitos fundamentais dos sujeitos passivos das investigações.

### 1.1 A interceptação de comunicações em massa e o caso *Big Brother watch and others v. The United Kingdom*

Em 13 de setembro de 2018, o Tribunal Europeu dos Direitos do Homem julgou o caso *Big Brother Watch and Others v. The United Kingdom.* Eduardo Bolsoni Riboli é quem utiliza o caso para se valer da análise do tema da conformidade do ordenamento jurídico do Reino Unido com a Convenção Europeia dos Direitos do Homem, em especial o programa de interceptação em massa do Reino Unido; a regulamentação sobre a partilha entre países e territórios estrangeiros de dados obtidos por agências de inteligência; e a regulamentação sobre a obtenção de dados de comunicações de provedores de serviços de comunicação. Tal decisão pode ser tomada como exemplo em matéria de investigação criminal, com potencial para impactar programas de vigilância

[139] *Ibidem.* Conforme *United States vs. Ladeau*, 2010 WL 1427523 (D. Mass, 2010).

de difentes países e seus ordenamentos jurídicos em relação ao regime de interceptação de comunicações.[140]

O caso diz respeito ao julgamento em conjunto de três queixas que foram feitas contra o Reino Unido pelos requerentes *Big Brother Watch* (organização britânica, apartidária e sem fins lucraticos, de proteção às liberdades civis e à privacidade), *English Pen* (entidade filantrópica que promove a liberdade de expressão), *Open Rights Group* (organização britânica de proteção e preservação dos direitos e liberdades digitais), Constanze Kurz (especialista em vigilância digital e porta-voz do grupo alemão "Computer Chaos Club", que realiza campanhas para demonstrar fragilidades em redes e programas informáticos que coloquem em risco interesses públicos, como o direito à privacidade), entre outras organizações. As queixas foram realizadas após as revalações de Edward Snowden em 2013, onde diversos documentos e informações confidenciais foram divulgadas sobre os programas de vigilância eletrônica globais operados pelos serviços de inteligência dos EUA e Reino Unido. Os requerentes alegaram crer que em razão do tipo de atividades por eles exercidas (relacionadas ao jornalismo, à defesa do direito de liberdade de expressão e defesa dos direitos humanos), os serviços de inteligência do Reino Unido haviam interceptado suas comunicações, seja pela interceptação direta pelos programas e sistemas de vigilância eletrônica do governo, seja por informações oferecidas por governos estrangeiros, como os Estados Unidos, ou seja por dados concedidos por serviços de comunicação.[141]

Assim, os requerentes passaram a questionar a legalidade da interceptação e obtenção de informações em massa e de modo oculto sobre os cidadãos ingleses e estrangeiros, principalmente através do monitoramento do trafégo da Internet. Uma das estratégias empregadas pelo governo do Reino Unido é a utilização do programa informático chamado TEMPORA, que, enre outras funções, permite a "interceptação em massa e gravação tradicional de comunicações telefônicas e a interceptação, coleta e análise do imenso volume de tráfego de dados que circulam pelos conglomerados de cabos de fibra óptica transoceânicos e continentais que estruturam a Internet e a criação de um índice, ou banco de dados, das informações obtidas"[142].

[140] RIBOLI, Eduardo Bolsoni. "*A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem*", in Galileu – Revista de direito e economia, Volume XIX, Lisboa, 2018, p. 53.
[141] *Idem*, p. 54.
[142] *Idem*, p. 55.

A partir disso, foi alegado violação do art. 8° da Convenção Europeia dos Direitos do Homem (o qual protege o respeito pela vida privada e familiar) pela lei britânica que regulava os poderes e medidas de interceptação na época (*Regulation of Investigatory Powers Act 2000 – RIPA,* atualmente revogada pelo *Investigatory Powers Act 2016).* Por mais que os requerentes tenham reconhecido que a interceptação em massa possua previsão legal no direito interno britânico, questionaram a *qualidade* da lei, referindo que sua complexidade tornava-a inacessível ao público, com preceitos "abaixo da linha d'água" (*below the waterline*) e carente de preceitos legais claros e garantias suficientes contra abusos. Alegaram, em específico, que a seção 8(4) da *Regulation of Invetigatory Powers Act* não observava os seis requisitos identificados pelo Tribubal Europeu dos Direitos do Homem no julgamento do caso *Weber and Saraiva v. Germany* (n° 54934/00), onde foi questionada a compatibilidade do sistema alemão de interceptação de comunicações telefônicas com a Convenção Europeia dos Direitos do Homem. Tais requisitos tratam-se da definição da categoria de pessoas que podem ter suas comunicações interceptadas; o limite de duração da medida; os casos de admissibilidade da interceptação de comunicações, em especial a natureza dos crimes que admitem este método de investigação; os procedimentos que devem ser observados na análise, uso e preservação dos dados obtidos; as precauções ao partilhar os dados com outras partes; e as situações que podem ou devem ser eliminados os dados que foram guardados.[143]

Em suma, os requerentes alegaram a evasividade e indefinição da Lei, dando margem a arbitrariedades, tendo em vista que os crimes que poderiam dar razão a medida não estavam suficientemente delimitados, bem como exisita a possibilidade de qualquer pessoa estar sujeita a ter suas comunicações interceptadas. Ainda, alegaram indefinição dos limites temporais da vigilância e carência de garantias adequadas quanto aos prodecimentos de análise, seleção e preservação dos dados interceptados. Alegaram também a desatualização dos requisitos do caso *Weber* mencionados acima, tendo em vista que foi julgado em 2006 e o acelerado desenvolvimento tecnológico permitiu ao Governo criar perfis detalhados e intrusivos aos aspectos íntimos da vida privada ao analisar padrões de comunicação a partir de uma interceptação em massa. Dessa maneira, entenderam pela necessidade da observância de três novos requisitos para conformidade da norma com Convenção Europeia dos Direitos do Homem: exigência

[143] *Idem,* p. 56.

de uma suspeita razoável das pessoas alvo das medidas; autorização judicial prévia; e subsequente notificação da vigilância.

Já o Governo do Reino Unido alegou que as informações e *intelligence* que estava obtendo eram essências para a proteção do Reino Unido contra ameaças á segurança nacional, principalmente, contra o terrorismo. Nas palavras de Riboli, o Governo apontou como argumento:

> "a sofisticação dos terroristas e criminosos e a assimilação das novidades tecnológicas às suas práticas criminosas, especialmente a utilização de medidas antiforenses como modo de impedir a detecção das suas atividades (através da criptografia ou então de programas e sistemas informáticos de comunicação personalizados). A imposição de novas garantias, reivindicadas pelos requerentes, prejudicaria a capacidade do Estado em garantir a segurança nacional e de combater crimes de especial gravidade, especialmente em uma era em que os avanços nas tecnologias de comunicação aumentaram a ameaça de terrorismo praticado através da Internet."[144]

Ainda, o requerido referiu que conforme a Conveção Europeia dos Direitos do Homem, cabe aos Estados avaliar as medidas necessárias para proteger a sociedade de ameaças, reforçando que as interceptações em massa (inclusive as promovidas na Internet) são essências para descoberta de ameças e de seus possíveis responsáveis. E por fim mencionou que as interceptações estavam previstas na *Regulation of Investigatory Powers Act* e que cumpriam os requisitos do caso *Weber*.

A decisão da corte partiu do entendimento de que a intervenção dos direitos previstos no art. 8° da Convenção Europeia dos Direitos do Homem somente é possível, ao abrigo do §2° do art. 8° da Convenção, se houver previsão legal e seja uma *providencia necessária, em uma sociedade democrática*, para alcançar os fins legítimos do §2° (a segurança nacional, a segurança pública, o bem-estar econômico do país, a defesa da ordem e a prevenção de infrações penais, a proteção da saúde ou da moral e a proteção dos direitos e das liberdades de terceiros). Por previsão legal, o tribunal tem entendido não somente por uma base legal específica que preveja a restrição de um direito, mas também pela clareza da lei, de modo que seja acessível aos cidadãos e previsível quanto aos seus efeitos, principalmente nos casos de vigilância secreta e meios ocultos de investigação (mas não no sentido de possibilitar ao sujeito vigiado saber anteriormente sobre a vigilância e adaptar sua conduta de maneira que julgar mais adequada, mas sim pela necessidade de minucioso e claro detalhamento das regras

[144] *Idem,* p. 57.

referentes à medida, visando proteger o indivíduo de arbitrariedades restritivas de direitos por parte das autoridades responsáveis pela investigação).[145]

Nessa linha, seguindo o seu entendimento de casos pretéritos, a Corte referiu que os Estados não necessitam tornar público todos os detalhes de um regime de vigilância secreta (as particularidades "abaixo da linha d'água" – *below the waterline*), justamente por serem características inerentes à atividade secreta, bastando que essas informações estejam disponíveis em domínio público. Já as disposições "acima da linha d'água" (*above waterline*) devem ser dotadas de previsibilidade, cumprindo os seis requisitos minímos estabelecidos no caso *Weber.*[146]

Da análise dos requisitos, a Corte entendeu que quanto á condição de previsibilidade, os Estados não são obrigados a nomear exaustivamente os crimes aos quais as medidas podem ser aplicadas, de modo que os termos "segurança nacional" e "crime grave" presentes na legislação britânica são suficientemente claros, permitindo ao cidadão saber em que situações as interceptações podem ser efetudas. Inclusive a Corte já havia se manifestado contra a excessiva rigidez do catálogo de crimes, tendo em vista que as aceleradas mudanças tecnológicas e socias dificultam a atualização legislativa e previsão das diferentes ameaças á segurança nacional. Já quanto ao segundo requisito, referente as pessoas sucetíveis de terem suas comunicações interceptadas, a Corte reconheceu que os cabos de fibra óptica interceptados não eram escolhidos de forma aleatória, dando preferência aos canais externos que tinham maior probabilidade de conduzir informações de interesse dos serviços de inteligência, não significando a interceptação da comunicação de todas as pessoas. Contudo, foi demonstrado preocupação com a ausência de *supervisão independente* dos identificadores e dos critérios de busca utilizados na filtragem das comunicações interceptadas, tendo em vista a possibilidade de irrestrita busca e exame de "dados de comunicação acessórios" (informações como a localização virtual ou física do equipamento interceptado, bem como identificação do remetente e do destinatário), já que diferentemente do conteúdo de uma comunicação que pode ser criptografado, os dados secundários não o podem, tendo potencial para revelar dados sensíveis dos participantes da comunicação. Portanto, neste termos, foi reconhecido que as

[145] *Idem*, p. 58-59.
[146] *Idem*, p. 59.

autoridades britânicas não efetuaram um justo equilíbrio entre os interesses públicos e os direitos individuais em conflito.[147]

Quanto aos limites temporais, foi considerado haver limitações bem definidas dos mesmos, de modo a evitar o abuso da medida, tendo em vista a previsão de seis meses para a investigação de crimes que atentem contra a segurança nacional ou econômica, e três meses para prevenção de crimes graves. Da mesma forma foram julgados adequados os procedimentos e precauções quanto ao tratamento dos dados obtidos (análise, uso e preservação). Os profissionais responsáveis pela análise das informações somente tinham acesso ao índice automaticamente criado pelos indicadores, ou seja, era afastada a análise dos matériais fora do índice, já que esses eram previamente descartados automaticamente. Além disso, os analistas somente estavam autorizados a examanir o conteúdo após a realização de um relatório elencando os motivos legitimadores para tal exame, demonstrando se a informação poderia ser obtida por outros meios de prova menos intrusivos. As garantias referentes ás precauções a serem tomadas na comunicação dos dados a outras partes também foram consideradas adequadas, bem como as disposições acerca da eliminação e destruição dos dados.[148]

Já no que se refere á proporcionalidade das interceptações em massa, embora este meio de investigação possa provocar graves restrições de direitos individuais, ele pode ser também considerado como uma valiosa estratégia para atingir os objetivos perseguidos, principalmente em virtude do atual nível de ameaça do terrorismo global e da criminalidade grave. Assim, a Corte entendeu que a medida é proporcional com base nos relatórios do *Independent Reviewer of Terrorism Legislation* (o qual apontou o perigo representado por ferramentas informáticas sofisticadas que impedem a detecção de atividades por meio tradicionais de investigação e alertou para a imprevisibilidade da rota de uma comunicação devido a natureza global da Internet).

Diante de tais considerações, o Tribunal concluiu que no caso *Big Brother Watch* as interceptações em massa foram realizadas dentro da margem de apreciação conferida aos Estados. Contudo, por mais que tenha reconhecido existir regulamentação sólida para esta modalidade de interceptação, demonstrou preocupação em duas áreas: ausência de supervisão de todo o processo de seleção, inclusive quanto a escolha dos cabos ou canais de comunicação a serem interceptados, os indicadores e critérios de

[147] *Idem*, p. 60-62.
[148] *Idem*, p. 63.

busca para a filtragem das comunicações interceptadas, e a seleção de material para exame por um analista; e ausência de salvaguardas aplicáveis na seleção de dados de comunicações acessórias para análise. Assim, em especial em razão de tais deficiências, o Tribunal Europeu dos Direitos do Homem considerou que o regime da seção 8(4) da *Regulation of Investigatory Powers Act* não cumpria ao requisito da *quality of law*, sendo portanto incapaz de manter a sua interferência no que é "necessário, em uma sociedade democrática", confirmando a violação do art. 8° da Convenção Europeia dos Direitos do Homem.[149]

A decisão do Tribunal pode ser considerada uma vitória do direito fundamental à privacidade perante os meios ocultos de investigação, já que reconheceu o elevado potencial intrusivo das interceptações de comunicação, seja na modalidade em massa ou direcionada. Contudo, pode-se dizer que o Tribunal falhou ao não aproveitar a oportunidade de atualizar os requisitos mínimos originados no caso *Weber* a serem observados na aplicação de uma medida de interceptação, como sugerido pelos requerentes.

## 2. Direito a inviolabilidade do domicílio

O direito fundamental à inviolabilidade do domicílio e da correspondência (e de outros meios de comunicação privada), está consagrado no artigo 34º da CRP e funciona como garantia do direito à reserva da intimidade da vida privada. Entende-se aqui por domicílio como

> "aquela área que tem por objecto a habitação humana, aquele espaço fechado e vedado a estranhos, onde recatada e livremente se desenvolve toda uma série de condutas e procedimentos característicos da vida privada e familiar, ou seja, um núcleo restrito sob o signo da intimidade, de protecção da vida privada, da liberdade e da segurança individual, onde se desenrola a vivência essencial, no aspecto existencial, da pessoa."[150]

A evolução dos valores/interesses que foram tutelados por meio do direito fundamental ao domicílio compreende, segundo Andrade, a paz do rei, patrimônio, privacidade, entre outros, mas a verdade é que sua proteção sempre foi contra a entrada (e permanência) arbitrária e indesejada de terceiros, visando garantir ao indivíduo o

[149] *Idem,* p. 64.
[150] Conforme Acórdão do Supremo Tribunal de Justiça de Portugal, de 20 de Setembro de 2009, proc. n.º 06P2321.

direito de ser deixado em paz. Nessa linha, a sua violação jurídica primordial sempre assumiu a forma de uma entrada/permanência *física* e *corpórea* por parte de pessoas indesejadas nas barreiras físicas representadas pelas paredes e telhados, de modo que somente se invadia a área de tutela desse direito fundamental se o agente entrasse física e arbitrariamente no espaço físico delimitado por tais barreiras.[151]

Contudo, os progressos técnico-científicos tornaram possíveis novas e diversificadas formas de intromissão e devassa á esfera da privacidade e intimidade que o direito quer proteger com a inviolabilidade do domicílio, que tem em comum o fato de não pressuporem a entrada e presença física ou corpórea do agente no espaço físico da habitação, mas que são passiveis de, sozinhos, exercer um drástico e irreversível sacrifício de valores. Como salientam Gomes Canotilho e Vital Moreira,

> "o domicílio não é violado somente quando se entra na morada de alguém sem o seu consentimento. Os modernos meios técnicos possibilitam a invasão do domicílio mediante meios electrónicos, que, além disso, permitem também a devassa das conversas e da vida privada dos moradores. A inviolabilidade do domicílio é seguramente incompatível com tais mecanismos."[152]

Dessa forma, a alternativa foi o a do alargamento da área de tutela do direito em questão. Percussor disso, o Tribunal Constitucional Federal alemão referiu que

> "ao tempo da elaboração da Lei Fundamental, o direito fundamental do artigo 13, I, da Lei Fundamental estava primacialmente voltado á defesa do titular do domicílio contra a indesejada presença física de um representante do Estado. Desde então surgiram novas possibilidades de colocação do direito fundamental em perigo. Os atuais dados técnicos permitem a intromissão na esfera espacial por outras formas. O fim da proteção da norma do direito fundamental resultaria frustrado se a proteção contra uma devassa da habitação com recurso a meios técnicos não fosse abrangida pela tutela garantida pelo artigo 13 da Lei Fundamental".[153]

Assim, novos comportamentos para além da entrada/permanência física passaram a ser considerados como violadores do domicílio, como a introdução e presença no domicilio de meios técnicos de escuta, de transmissão de imagens ou de sons, ou até por meios de captação á distância, onde o dispositivo não precisa necessariamente estar inserido dentro do domicilio, mas o seu uso permite saber o que

[151] ANDRADE, Manuel da Costa. 2009, p. 151.
[152] CANOTILHO, J.J. Gomes e MOREIRA, Vital. 2007, p. 540.
[153] ANDRADE, Manuel da Costa. 2009, p. 151-152.

se passa e o que é dito dentro das quatro paredes. De acordo com o Tribunal Constitucional Federal,

> "agressão é toda a forma de observação ou vigilância óptica ou acústica do espaço da habitação, seja ela realizada com meios técnicos introduzidos no interior do espaço protegido, seja com meios colocados no exterior".[154]

Portanto, é decisivo apenas que a devassa recaia sobre o próprio espaço fisicamente delimitado da habitação e que, dessa maneira, haja ainda uma ultrapassagem das barreiras físicas (paredes e telhados), mesmo que sem a entrada (e presença) física do agente, o que pode ser realizado através da utilização de microfone direcionado que permite, mesmo que no exterior da habitação, escutar, gravar, fotografar, pessoas e palavras ditas no interior.[155]

Dito isto, cabe analisar que houve (e ainda há) muita discussão doutrinaria e jurisprudencial sobre a admissibilidade das escutas de conversas em domicilio privado, principalmente na Alemanha, onde esses casos são chamados de "grande espionagem acústica", enquanto que as escutas de conversas fora do domicilio privado são denominadas de "pequena espionagem acústica". As críticas a tal medida se justificam, segundo Roxin, principalmente pelo fato de que ela não apenas afeta pontualmente a esfera privada (como nos casos de escutas telefônicas), mas sim a suprime por completo, onde toda manifestação acústica da vida (até a que ocorre dentro do dormitório) é controlada pelo Estado, considerando-se um verdadeiro ataque contra a dignidade humana.[156]

Desse modo, até 1998 o domicilio era inviolável e não se previa exceção alguma para as escutas domiciliares. Contudo, no mencionado ano foi introduzido um novo parágrafo 3º no art. 13º da Constituição alemã que previu que quando determinados feitos fundem a suspeita de que alguém tenha cometido um fato punível particularmente grave, assim determinado por lei, poderia ser utilizado na persecução do feito, em virtude de uma ordem judicial, meios técnicos para a vigilância acústica do domicilio em que presumivelmente se encontre o imputado, se por outro modo de investigação a resolução do feito for excessivamente mais difícil ou não ofereça probabilidade alguma de êxito. A medida deve ser sujeita a prazo e a ordem deve ser decidida por um tribunal

[154] *Idem*, p. 152.
[155] *Ibidem.*
[156] ROXIN, Claus. *"La protección de la persona en el derecho processal alemán",* em *La evolución de la política criminal, el derecho penal y el proceso penal*, Valencia: Tirantlo Blanch, 2000, p. 155.

integrado por três juízes. Em caso de perigo de demora, a medida pode também ser ordenada por um único juiz.[157]

Com base nessa reforma constitucional, no mesmo ano foi introduzido no Código de Processo Penal alemão, por meio de uma Lei para melhorara da luta contra a criminalidade organizada, um novo §100c, parágrafo 1º, nº 3, autorizando a escuta de conversas em domicílios para uma lista enorme de feitos puníveis, que com frequência são cometidos em relação com a criminalidade organizada.[158]

Não demorou muito para que a discussão sobre a admissibilidade da "grande espionagem acústica" chegasse ao Tribunal Constitucional Federal, que entendeu, em princípio, que ela não é inadmissível, mas que deve sofrer alterações para que seja protegida a dignidade humana e o princípio da proporcionalidade, abarcada pelo princípio do Estado de direito. No que se refere à dignidade humana, o Tribunal baseou-se na sua "teoria do âmbito essencial da vida privada", a qual já foi mencionada aqui. Á intangibilidade da dignidade humana pertence o reconhecimento de um âmbito essencial da configuração da vida privada, absolutamente protegido. Nesse âmbito não pode intervir a vigilância acústica da residência em vista dos fins da persecução penal. Ou seja, não há lugar para uma ponderação entre o interesse da persecução penal e o interesse da inviolabilidade do domicilio. Portanto, quando a escuta conduz a obtenção de informações do âmbito essencial de configuração da vida privada, ela deve ser interrompida, e se caso já tenha gravado algo, as gravações existentes devem ser excluídas (qualquer valoração de tais informações está excluída). Na prática, isso significa para o Tribunal Constitucional Federal que não podem ser feitas escutas quando o imputado se encontra no domicilio acompanhado somente dos seus familiares mais próximos e que não existem indícios da participação dos mesmos no fato em investigação. Mas quando as conversas sobre os feitos puníveis sejam mantidas com cumplices, ainda que eles sejam de estreita confiança do imputado, é possível a gravação das mesmas, mas mesmo assim respeitando quaisquer manifestações que digam respeito ao âmbito essencial da vida privada.[159]

Outra limitação proposta pelo Tribunal, derivada do princípio da proporcionalidade, foi a de que as escutas somente devem ser permitidas para feitos puníveis especialmente graves (e não como havia sido previsto no §100c, parágrafo 1º,

[157] ROXIN, Claus. 2008, p. 75.
[158] *Ibidem.*
[159] *Idem,* p. 76-78.

nº 3, do Código de Processo Penal, que previa a mesma para investigação no âmbito da "criminalidade media", abarcando um grande leque de crimes). Assim, entendeu-se que a mesma deve ser admitida apenas para crimes onde está prevista uma pena privativa de liberdade máxima superior a cinco anos, como por exemplo, o homicídio.[160]

Contudo, dois membros da Sala do Tribunal (de um total de oito membros, por tanto, uma minoria não determinante para a decisão) entenderam pela inadmissibilidade absoluta das escutas em domicilio, considerando a grande espionagem acústica inconstitucional em todos os casos. Em favor da proteção da possibilidade de expressar-se de forma livre e pessoal, e para salvaguarda da dignidade humana, se deve supor em todo caso para os domicílios privados que esses oferecem um espaço para comunicação pessoal e podem ser utilizados para esse fim, não devendo haver escutas nos mesmos. Aos indivíduos deve ser dada a possiblidade de expressar sucessos, sentimentos, reflexões, opiniões e experiências intimas sem medo de serem observados por instituições públicas. Ainda, referiram que as proibições de valoração somente oferecem uma "proteção insuficiente", não podendo fazer de conta que o conhecimento dos conteúdos que fazem parte do âmbito essencial da vida privada não irá influenciar as autoridades da persecução penal contra o suspeito ou até mesmo contra terceiros. Da mesma forma, as autoridades da investigação dificilmente poderão controlar dia e noite cada uma das conversas que são objeto de vigilância, e tão pouco poderão identificar com quem o suspeito está falando, se é um familiar ou um cumplice.[161]

O mestre Claus Roxin compartilha dessa opinião minoritária e contrária, referindo:

> "Pues ya el temor de que personas sospechosas y no sospechosas podrían ser espiadas en el ámbito más privado destruye la sensación de encontrarse en una esfera protegida, en la cual el Estado Leviathan no puede penetrar."[162]

Mas apesar da divergência existente, concluiu-se pela admissibilidade da intervenção acústica no domicilio, mas somente nos casos em que possa presumir-se que estão ocorrendo acordos conspiratórios na residência privada. Ainda, as conversas com pessoas de estreita confiança do suspeito, especialmente familiares e companheiros

[160] *Idem,* p. 78.
[161] *Idem,* p. 78-79.
[162] ROXIN, Claus. 2008, p. 79.

sentimentais, devem seguir sendo um tabu, ainda quando eventualmente possam ser manifestadas expressões autoincriminatórias de um delito já cometido.

A discussão e decisão do tribunal exposta acima pode ser aplicada também para os casos de ativação, através da Internet, da câmara ou microfone de um computador situado dentro de casa e que, por essa via, se torne possível escutar e observar o que ocorre no interior da habitação (o que é possibilitado via utilização de *malware/buscas online*, que será tratado posteriormente). Trazendo de volta o entendimento de Andrade, de uma forma geral, o acesso de forma oculta e à distância via *malware* permite também que os dados contidos no computador visado sejam observados, e se necessário for, copiados em maior ou menor medida. Isso pode acontecer sob a forma de intromissão instantânea e descontinua (*espelho*) ou de forma contínua, permitindo o registro das alterações ocorridas no computador-alvo (*monitoring)*.[163]

Todavia, existe uma divergência doutrinal se as *buscas online* atingem a área de tutela do domicilio ou não (isto para os casos em que o computador atingido se encontra no domicílio do utilizador)[164]. Mas assim como acontece na entrada física não consentida, entende-se que aqui também se viola o domicílio, entendido como o "último refúgio" espacial para a expressão da privacidade e da intimidade. Pois do mesmo modo, aqui também resta frustrada a expectativa de entrincheiramento dentro das quatro paredes e se acessa a dados que, de outra forma, só a custa da entrada arbitrária no domicílio seria possível alcançar. Nesse sentido, Costa Andrade[165] expõe a situação com clareza quando refere que do ponto de vista da tutela da privacidade, independe se alguém guarda os seus segredos em um diário no armário do seu quarto ou em um texto gravado no seu computador situado no mesmo quarto. Nada justifica um tratamento diferenciado para o acesso indevido do diário pela entrada indevida no quarto ou pelo recurso ás técnicas de *hacker*[166].

[163] ANDRADE, Manuel da Costa, 2009, p. 152.
[164] De salientar que há na doutrina discussão se a busca online que atinja um computador portátil, onde quer que ele se encontre, estaria também violando o domicílio. Para MANUEL DA COSTA ANDRADE, 2009, p. 154, "numa consideração teleológico-racional das coisas, não pode adscrever-se relevo decisivo á circunstância puramente fortuita do lugar onde o computador se encontra".
[165] ANDRADE, Manuel da Costa, 2009, p. 154.
[166] Em informática, hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um hacker frequentemente consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento "normal" dos sistemas como previstos pelos seus criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados. Informações retiradas do site: https://pt.wikipedia.org/wiki/Hacker. Acesso em 22/09/2017.

Portanto, pelo exposto aqui, é indiscutível que o domicílio está exposto a novas formas de invasão e devassa, que não representam a entrada e permanência físicas arbitrárias, mas nem por isso são portadoras de menor danosidade. Muito pelo contrário, pelo caráter oculto das novas formas de invasão e espionagem proporcionadas pelo avanço tecnológico, a inviolabilidade do domicílio passou a correr novos e maiores riscos.

## 3. O princípio da não autoincriminação (n*emo tenetur se ipsum accusare*)

Pertencente aos princípios internacionalmente reconhecidos do processo penal de um Estado de Direito, o princípio da não autoincriminação (*nemo tenetur se impsum accusare)* garante que ninguém é obrigado a autoincriminarse ou produzir prova contra si mesmo. Nenhum indivíduo pode ser obrigado, por qualquer autoridade ou mesmo por um particular, a fornecer involuntariamente qualquer tipo de informação/prova que o incrimine direta ou indiretamente. Assim, qualquer tipo de prova contra o réu que dependa ativamente dele, somente valerá se o ato for levado a cabo de forma voluntária e consciente, sendo intolerável a fraude, a coação física ou moral, a pressão, etc.[167]

Mas como muito bem exposto por Roxin, o princípio *nemo tenetur* não busca apenas evitar que se valorem provas obtidas mediante coação e tortura, mas também impedir que se admitam provas obtidas mediante outro tipo de manobras enganosas, obviamente menos brutais que as coativas, mas que igualmente infringem a proibição de autoincriminação, como a obtenção de uma confissão do imputado introduzindo na sela prisional do mesmo um agente policial encoberto para obter essa informação, ou a gravação das conversas do visado com pessoas da sua confiança em um local privado.[168]

Um exemplo que pode ser trazido aqui para demonstrar a área de tutela do direito em tela é o caso do "interrogatório ardil", onde a polícia contata uma pessoa do círculo de confiança do imputado (um amigo, por exemplo) e o induz a chamar o suspeito por telefone e o envolve em uma conversa sobre o fato em investigação, possibilitando que sejam obtidas manifestações autoincriminatórias. A polícia escuta toda a conversa entre os indivíduos e utiliza as manifestações do imputada para provar sua culpabilidade.[169]

[167] ROXIN, Claus. 2008, p. 28.
[168] *Idem*, p. 28-29.
[169] *Idem*, p. 61.

Existem duas posturas dentro do Supremo Tribunal Federal alemão sobre a legitimidade e admissibilidade das provas obtidas dessa maneira. A 5ª Sala entendeu ser proibido um procedimento de tal índole e invalorável uma declaração obtida dessa maneira. A decisão foi fundada na tese de que o direito á permanecer calado, bem como a sua instrução ao imputado, restaram ofendidos. O princípio *nemo tenetur* não só proíbe a coação, mas também pretende proteger o imputado de uma autoincriminação induzida pelo Estado por meio do erro e da manipulação. [170]

Por outro lado, há membros do Tribunal que limitam o princípio em tela a evitar uma coação para declarar, visando impedir apenas que o imputado, por erro, se considere obrigado a declarar, entendendo ser permitido utilizar as provas obtidas por esse meio. A 2ª Sala do Supremo Tribunal Federal se manifestou da seguinte maneira:

> "La libertad del imputado de manifestarse sobre la imputación o de permanecer callado (principio *nemo tenetur*...) no ha sido (...) afectada. El que se expressa frente a una persona particular sobre el hecho imputado no puede dudar de la libre voluntad de esa conducta..."[171].

Em razão da divergência entre as Salas, o caso chegou a "*Gran Sala*", que entendeu, em um primeiro momento, que a obrigação legal de instruir somente quer assegurar que o imputado seja preservado da suposição errônea de que existe uma obrigação de declarar. Nesse sentido, não há lesão quando uma pessoa particular, ainda que por iniciativa das autoridades de investigação, envolva o suspeito em uma conversa e obtêm manifestações através das quais o autoincriminem. Contudo, por último, a *Gran Sala* entendeu que o comportamento das autoridades no caso em tela, ainda que não tenham praticado uma coação, faz o caráter secreto da medida aproximar-se muito de uma lesão do princípio *nemo tenetur* e do "princípio de um procedimento levado a cabo com lealdade". Em razão disso, concluiu-se que o "interrogatório ardil" somente pode ser admissível quando se trata de feitos puníveis de "importante significado" e quando com a utilização de outros métodos de investigação a averiguação dos fatos seria muito menos promissora ou seria consideravelmente mais complicada.[172]

Mas para o mestre Roxin, a idéia do interrogatório ardil deveria ser absolutamente proibida, independentemente da gravidade do feito e da maior ou menor complexidade das investigações ou de qualquer outra característica do caso, pois tal

[170] *Idem*, p. 62.
[171] *Ibidem.*
[172] *Idem*, p. 64.

medida significa iludir a lei, não informando o imputado dos seus direitos. Pois se o imputado ao menos sabe que está sendo interrogado, tentará organizar suas declarações de uma maneira que elas não o incriminem, ou que incriminem o menos possível. Porém, se um terceiro o faz crer que não esta na frente da polícia, ou até que pretende ajudá-lo com o caso, o imputado revelará muito mais sobre aquilo que em virtude da lei poderia calar.[173]

O caso citado acima pode facilmente ser abordado a partir de uma perspectiva de ocorrência no ambiente digital, adequando-se melhor ao nosso estudo. A conversa entre o suspeito e a pessoa de sua confiança poderia muito bem ter ocorrido via *Internet*, por meio dos mais variados serviços de comunicação oferecidos, onde as autoridades investigadoras acompanhariam toda comunicação junto da pessoa de confiança do suspeito, da mesma forma como se fosse por telefone.

Em Portugal tal meio é admissível e intitulado pela doutrina como *terceiro infiltrado* (o qual é utilizado também, com frequência, nos EUA), de modo que quando se revela particularmente difícil ou mesmo inviável a infiltração de um agente encoberto da polícia em um meio criminoso ou para a interação particular com um suspeito, pode ser necessário recorrer a um civil que pelos seus contatos, conhecimentos específicos ou pelo fato de já estar integrado no meio sob investigação, poderá recolher as informações pretendidas.[174]

No âmbito da investigação criminal em ambiente digital, acrescenta Ramalho, o recurso a terceiros é especialmente útil quando se trata de um terceiro integrado no meio criminoso ou um terceiro cujos especiais conhecimentos técnicos lhe permitem infiltrar-se em áreas que, de outro modo, permaneceriam inacessíveis a agentes encobertos da policia, como por exemplo, nos casos popularizados nos EUA dos *hackers* contratados pela polícia para utilização dos seus conhecimentos para fins legítimos (é o que se chama a conversão de um *black hat hacker* em *white hat hacker*).[175]

Por outra senda, outro caso onde levanta-se a discussão sobre a violação ou não do princípio *nemo tenetur*, é um caso onde foram gravadas as conversas do suspeito com seus familiares por meio da utilização de aparatos de escutas á distancia, as quais poderiam, por analogia, serem comparadas com o já referido recurso á *malware.*

[173] *Idem*, p. 67.
[174] RAMALHO, David Silva, 2017, p. 298-299.
[175] *Idem*, p. 299.

O caso em questão também ocorreu na Alemanha, onde o acusado negou haver cometido o crime do qual era imputado. Tratava-se de um incêndio especialmente grave onde dez pessoas haviam perdido a vida. Dessa forma, passaram a ser gravadas as conversas que o mesmo manteve com seus parentes em um lugar destinado a receber visitas no estabelecimento penitenciário (o que difere do tratado anteriormente sobre o domicilio), sem nem ele ou seus parentes terem conhecimento disso. As informações obtidas nessas ocasiões contribuíram posteriormente para provar a sua culpabilidade e condenação.[176]

Segundo o Processo Penal alemão, é previsto que a palavra não pronunciada publicamente pode ser escutada e gravada por meios técnicos quando, como no caso em questão, existe a suspeita do cometimento de um feito punível determinado, especialmente grave, e quando sem o emprego de um aparelho de escuta a distância as investigações não ofereceriam possibilidade alguma de êxito ou seriam consideravelmente mais difíceis, e, sempre, deve existir uma ordem judicial para tanto.[177]

Essa situação é diferente do interrogatório ardil onde o Estado obtém manifestações autoincriminatórias por meio de enganos e de outros métodos que afetam a voluntariedade do imputado, pois aqui unicamente se "espia" comunicações que o imputado realiza por iniciativa própria. Portanto, entende-se que nesses casos não existe uma lesão ao princípio *nemo tenetur*, pois o Estado não ocasiona a autoincriminação, mas somente escuta e tira proveito dela. Todavia, como seria de se imaginar pelo que já tratamos até aqui, a valoração de tais gravações podem ser problemáticas por outro motivo, tendo em vista que podem atingir o âmbito essencial de configuração da vida privada. Assim, ainda que no presente caso das gravações não se visualize ofensa ao princípio *nemo tenetur* (ainda mais pelo fato de o Tribunal alemão ter entendido que a sala de visitas da prisão não constitui um âmbito privado e que pode ser vigiada), deve-se ter muito rigor por parte dos agentes envolvidos nas escutas para que não se lesione esse âmbito essencial da vida privada, devendo tais manifestações serem subtraídas da valoração no processo penal toda vez que vierem ao conhecimento dos agentes, sendo imediatamente excluídas (como visto anteriormente).[178]

[176] ROXIN, Claus, 2008, p. 72.
[177] *Ibidem.*
[178] *Idem*, p. 72-73.

Mas entende-se que distinto seria se também fossem colocadas escutas na cela de prisão de um detento que a compartilhe com um ou vários detentos. Pois neste caso a pessoa encarcerada pelo Estado não teria nenhum outro lugar no mundo onde poderia falar sem perigo sobre aquilo que á atormenta, restando seus direitos violados e as informações assim obtidas inadmitidas como prova.[179]

De maneira semelhante, um fato ocorrido na Alemanha em 1998, onde a 3ª Sala decidiu um caso em que na cela de um detido em prisão preventiva foram sequestradas anotações feitas pelo mesmo para fins de sua defesa. As manifestações feitas por ele sobre o fato foram utilizadas pelo tribunal estadual para provar sua culpabilidade. Após, o Supremo Tribunal Federal declarou, com razão, a inadmissibilidade de tal prova e a revogação da sentença com base no "direito a uma defesa efetiva", e com base na violação do "direito a permanecer calado do imputado" (*nemo tenetur*). Ainda, o Tribunal entendeu pela inadmissibilidade de tal prova pois aqui não se trata de objetos materiais como elementos probatórios (como seria a arma utilizada para cometer o delito ou um documento falsificado), mas sim de uma manifestação dos pensamentos do imputado destinada somente a ele mesmo, não comunicativa. Tampouco existe, como ocorre nas escutas secretas, uma comunicação ao mundo exterior, tratando-se tão somente de fixar pensamentos próprios. Assim, se as utiliza contra o acusado, ás emprega como uma exteriorização comunicativa que o mesmo nunca quis fazer.[180]

Portanto, conclui-se com base nas lições da jurisprudência alemã, que não serão todos os casos de ingerência estatal de forma oculta que acarretarão na violação do princípio *nemo tenetur* e na inadmissibilidade das provas assim obtidas, dependendo sempre da análise do caso concreto e de um juízo de proporcionalidade, de modo que, como visto, ainda que haja uma certa influência das autoridades estatais para a ocorrência de uma autoincriminação, poderão ser admitidas tais declarações como prova quando a peculiaridade e gravidade do caso assim o exija.

## 4. A criação do direito fundamental à confidencialidade e integridade dos sistemas informáticos e das *buscas online* como meio de obtenção de prova na Alemanha

Outro direito fundamental que merece destaque quando se fala da utilização de métodos ocultos de obtenção de prova, e esse em específico quando as investigações

[179] *Idem*, p. 73.
[180] *Idem*, p. 74.

ocorrem em ambiente digital, é o *direito fundamental à confidencialidade e integridade dos sistemas informáticos*, o qual teve seu recente nascimento na Alemanha em razão da pretensão da criação de uma lei que permitisse a utilização das já mencionadas buscas online (*malware*).

Tudo começou em 2006, quando no contexto de uma investigação criminal relacionada com a prática de atos terroristas, um Procurador da República requereu um mandado judicial para instalar um *Trojan* no computador do suspeito e assim realizar uma pesquisa remota, utilizando-se do termo *busca online.* Em 25 de novembro de 2006 o pedido foi negado sob os fundamentos de falta de previsão legal da medida investigatória e pelo princípio da proibição de analogia no direito penal. Inconformado, o Procurador interpôs recurso para o Tribunal de Justiça Federal da Alemanha, alegando que as normas do Código de Processo Penal alemão referentes à busca em locais físicos permitiria o recuso à desejada busca online. A decisão de primeiro grau foi confirmada pelo Tribunal, que entendeu que a analogia entre os dois tipos de busca improcedia e que, consequentemente, inexistia previsão legal que permitisse conceder o mandado requerido.[181]

Todavia, menos de um mês depois dessa decisão, o Estado Federado de Nordrhein-Westfalen altera a sua Lei de Proteção da Constituição e introduz no seu § 5.2(11)[182] uma norma que vem permitir à entidade responsável pela proteção da Constituição realizar as ditas buscas online, legitimando o acesso secreto a sistemas informáticos, com recurso à exploração de vulnerabilidades técnicas, para a instalação de *malware*, e conferindo à referida autoridade a possibilidade de espiar, monitorar, analisar o conteúdo e até controlar o sistema informático afetado. Tal medida só poderia ser utilizada em casos relativos a atividades ilícitas que ameaçassem a livre ordem democrática fundamental ou a continuada existência ou segurança da Federação, de uma *Land* ou dos respectivos membros.[183]

---

[181] As informações sobre este caso que constam nas próximas páginas foram retiradas da obra RAMALHO, David Silva, 2013, p. 216-219. E para maiores informações sobre o caso, acessar: http://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php. Acesso em: 04/01/2018.

[182] A norma prevê o seguinte: "(2) De acordo com o §7, a autoridade para proteção da Constituição pode aplicar as seguintes medidas para adquirir informação como meio de serviço de *intelligence*: [...] 11. Monitorização secreta e outro reconhecimento da Internet, como em particular participação encoberta nos seus meios de comunicação e de pesquisa, bem como acesso secreto a sistemas informáticos envolvendo a instalação de meios técnicos. Na medida em que tais medidas constituam uma ingerência no segredo da correspondência, correio ou telecomunicações ou seja equivalente a tal ingerência em termos de natureza e gravidade, está será apenas admissível sob as condições do artigo 10 da Lei Fundamental".

[183] RAMALHO, David Silva. 2013, p. 217.

Pouco tempo após sua edição, cinco cidadãos alemães que foram afetados pela norma e consequentemente pelo meio de obtenção de prova previsto pela mesma, requereram a sua apreciação pelo Tribunal Constitucional Federal Alemão. O Tribunal analisou a questão a partir da análise de direitos fundamentais como o direito à privacidade da correspondência, do correio e das telecomunicações; o direito à inviolabilidade do lar; o direito à autodeterminação informacional; e o direito ao livre desenvolvimento da personalidade. Entretanto, da análise detalhada de cada um destes preceitos constitucionais, o Tribunal concluiu que os mesmos eram insuficientes para conferir proteção em relação ao meio de obtenção de prova em apreço.[184]

Dessa maneira, deparado com a inexistência de normativas suficientes para a proteção do sistema informático dos investigados, bem como dos dados armazenados e transmitidos pelo mesmo, o Tribunal criou, por via jurisprudencial, o *direito fundamental à confidencialidade e integridade dos sistemas informáticos*. Esse direito fundamental é criado com base na dignidade da pessoa humana e no direito ao livre desenvolvimento da personalidade, tendo o objetivo último de proteger a vida privada dos cidadãos contra o ingresso do Estado nos sistemas informacionais, principalmente quando pode-se acessar o sistema como um todo e obter os mais variados dados sobre a personalidade do visado, sendo obrigatória a existência de uma maior proteção, ainda mais nos casos em que tal intromissão possa ocorrer de forma oculta.[185]

O Tribunal germânico entendeu pela insuficiência do direito fundamental da inviolabilidade do domicílio para conferir proteção em relação ás buscas online, pois entende que tal proteção alcançaria apenas os dados armazenados em sistemas informáticos situados fisicamente dentro do domicílio do investigado, excluindo os atuais dispositivos moveis que podem ser utilizados em qualquer lugar e que da mesma forma contam com uma elevada capacidade de armazenamento de dados (*notebooks, smartphones, tablets*, etc.). Dessa maneira, o Tribunal refere que a inviolabilidade do domicílio seria suficiente para proteger aquela infiltração secreta a um equipamento informático que requeira um acesso físico prévio ao domicilio do suspeito por parte dos agentes para manipular fisicamente o sistema informático. Ou, quando com a infiltração secreta no sistema informático que se encontra em um domicilio se pretenda controlar o que acontece no interior do mesmo, mediante a ativação do microfone ou webcam do

[184] *Ibidem.* E conforme acordão BverfG, do Primeiro Senado, 1 BvR 370/07 e 595/07, de 27 de fevereiro de 2008, disponível em http://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em: 04/01/2018.
[185] RAMALHO, David Silva, 2013, p. 218.

sistema informático visado. Porém, Pradillo defende que nos casos da busca online não é necessária uma intromissão física dos investigadores no domicílio ou no lugar onde o sistema informático se encontre, podendo acessar o mesmo por via remota mediante o envio de um *software* específico, como veremos mais a frente.[186]

Na mesma linha, advertiu o Tribunal pela insuficiência do direito fundamental ao segredo das comunicações, ao ponto que tal direito protege os cidadãos frente ao conhecimento, por parte de terceiros, acerca da existência de uma comunicação, do seu conteúdo e das suas circunstâncias, mas não protege a confidencialidade e integridade dos equipamentos informáticos, já que com a medida consistente no registro online de tais equipamentos não se pretende exatamente interceptar uma comunicação, mas sim acessar, através das vias de comunicação existentes, ao interior de um equipamento informático com o objetivo de conseguir seu controle e inspecionar o conteúdo do mesmo.[187]

É de se louvar o entendimento do Tribunal de que a proteção desse direito fundamental se mantém independentemente da capacidade de armazenamento de dados pessoais ser ou não utilizada no caso concreto, pois o que se protege é, efetivamente, o sistema informático em si e a susceptibilidade de este conter dados sensíveis, nomeadamente dados pessoais. Assim, pode-se dizer que esse novo direito fundamental visa garantir ao utilizador que os dados criados, processados e armazenados pelo seu sistema informático permanecerão efetivamente confidenciais, e que esse mesmo sistema informático terá a sua integridade mantida. E de fato, as singularidades impostas pela evolução tecnológica estão demandando da jurisprudência uma atenção renovada que supere os enclaves históricos, exigindo a criação de novos direitos fundamentais capazes de oferecer proteção frente aos novos mecanismos tecnológicos utilizados em investigações criminais. E por não existir um horizonte cerrado das evoluções tecnológicas, que estão em permanente e constante avanço, é obrigatório um renovado entendimento como o do Tribunal Alemão das exigências que motivam as resoluções judiciais que habilitam qualquer ato de ingerência na privacidade dos investigados.[188]

---

[186] PRADILLO, Juan Carlos Ortiz. "*Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos",* em *El derecho en la sociedad telemática: estudios en homenaje a Valentín Carrascosa López*, (coord. Marcelo Bauzá Reilly, Federico Bueno de Mata), Santiago de Compostela: Andavira Editora, 2012, p. 57-86.
[187] *Ibidem.*
[188] RAMALHO, David Silva. 2017, p. 247.

Apesar de ainda pouco desenvolvida na doutrina e na jurisprudência portuguesa, a integridade dos sistemas de informação tem sido invocada como sendo o bem jurídico tutelado pelo crime de falsidade informática (artigo 3.º Lei do Cibercrime – Lei nº 109/2009, de 15 de setembro), através do qual se

> "pretende impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados."[189]

Contudo, esse entendimento não é unânime. Como exemplo disso, cita-se o Acórdão do Tribunal da Relação de Évora, de 19 de Maio de 2015, em que se considera que o crime de falsidade informática visa

> "proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos."[190]

Mas voltando à experiência Alemã sobre a questão, o Tribunal não considerou o direito fundamental à confidencialidade e integridade dos sistemas informáticos como ilimitado, admitindo sua restrição, por motivos de perseguição e prevenção criminal, quando a sua violação fosse justificada. Os requisitos para que tal restrição ocorra (e consequentemente seja possível a utilização das ditas buscas online) devem ser definidos em lei (que também deverá prever medidas para proteger a área central da vida privada), além do necessário controle judicial e a limitação para ser utilizado apenas quando se está diante de uma ameaça específica. Ou seja, quando em um caso concreto haja uma probabilidade razoável de que, se não houver uma intervenção do Estado, no futuro se produzirá um dano contra um interesse jurídico predominantemente importante, sendo destacada a importância da saúde, da vida, e da liberdade, ou em caso de ameaça pública à própria raiz ou existência do Estado. Após essas considerações feitas pelo Tribunal Constitucional Federal (que sem dúvida eram as coordenadas para que uma futura formulação legal sobre o uso de *malware* como meio de obtenção de prova se coadune com os imperativos constitucionais violados), o mesmo concluiu que a norma criada pelo Estado Federado de Nordrhein-Westfalen também violava os

[189] Acórdão do Tribunal da Relação de Lisboa de 30 de Junho de 2011, proc. n.º 189/09.3JASTBL.L1-5 e Acórdão do Tribunal da Relação do Porto de 24 de Abril de 2013, proc. n.º 585/11.6PAOVR.P1.
[190] Acórdão do Tribunal da Relação de Évora, de 19 de Maio de 2015, proc. n.º 238/12.8PBPTG.E1.

princípios da clareza e certeza legal e da proporcionalidade, concluindo pela sua inconstitucionalidade.[191]

Segundo o princípio da clareza, previsto no parágrafo 20 e 28.1 da *Grundgesetz* (que representa a Constituição alemã), é assegurado que as ações levadas a cabo pelas autoridades nacionais encontrem limites estipulados na lei, suficientemente determinados e claros, de forma que não gerem arbitrariedades na sua interpretação e aplicabilidade. Já no que se refere a violação do princípio da proporcionalidade, o Tribunal referiu que as medidas adotadas pelo Estado ao aplicar a norma em causa não se coadunaram com a exigência de adequação, necessidade e proporcionalidade, já que a medida, segundo expresso na lei, se limitava à luta contra o terrorismo, mas acabou sendo utilizada em situações diversas. Assim, tendo presente as referidas coordenas oferecidas pelo Tribunal, e considerando que as buscas online se revelam como um meio necessário e adequado para obtenção de prova quando utilizado de forma proporcional (na perspectiva de que a gravidade da intrusão não é necessariamente maior do que a gravidade da razão pela qual ela é realizada), em 25 de dezembro de 2008, através da Lei para Defesa face aos Perigos do Terrorismo Internacional, é introduzido no ordenamento jurídico alemão a possibilidade, a título excepcional, do uso de *malware* para efeitos de prevenção/investigação de crimes de terrorismo.[192]

E de fato, a proliferação de ameaças terroristas contra o Estado de Direito faz com que seja necessário o sacrifício de determinados direitos fundamentais para que a defesa e segurança dos cidadãos e do Estado sejam garantidas, e para que isso ocorra, é obrigatório ao Estado atualizar os seus meios legais e tecnológicos de prevenção e de obtenção de prova. Mas de qualquer maneira, e ainda mais se estamos perante uma medida secreta de vigilância realizada por um órgão estatal, o núcleo essencial da vida privada deve ser respeitado e jamais violado, já que aí se incluem a possibilidade de expressar acontecimentos internos, como percepções e sentimentos, bem como considerações, opiniões e experiências de uma natureza altamente pessoal, e que podem estar armazenadas em sistemas informáticos, não sendo admissível aos cidadãos temer que organismos estatais tenham acesso a essas informações. Dessa maneira, e com a intenção de cumprir com os requisitos estabelecidos pelo Tribunal, a Lei em questão, além de prever a necessidade de autorização judicial expressa e a existência comprovada de um perigo concreto para bens jurídicos de particular importância (o que

[191] RAMALHO, David Silva, 2017, p. 248.
[192] *Idem*, p. 249.

demonstra o caráter excepcional da medida aos casos de prevenção de terrorismo), também fez a previsão de normativos que protejam o núcleo essencial da vida privada do investigado.[193]

Por exemplo, os dados coletados na investigação são disponibilizados para análise pela Comissão de Proteção de Dados, e caso se deparem com dados referentes ao núcleo central da vida privada do investigado, esses deverão ser eliminados imediatamente. Ainda, o parágrafo 3º da Lei prevê que sempre que se recorra à medida em causa, deverá ser registrado o meio técnico utilizado, a duração do procedimento, as características do sistema informático visado, as mudanças efetuadas, informações que permitam a identificação dos dados recolhidos, a unidade que executou a ação, entre outras informações. Essa descrição da ação permite que posteriormente a pessoa visada examine se a medida ocorreu em conformidade com as exigências legais, garantindo também o contraditório e ampla defesa. Importante referir também, que a ordem para a medida deverá, em regra, ser limitada ao prazo máximo de três meses.[194]

Sendo assim, a referida Lei parece legitimar de uma maneira adequada e suficiente o uso de *malware*, sendo um ótimo exemplo a ser seguido pelos demais ordenamentos jurídicos. Além disso, se mostra de grande importância a herança jurisprudencial deixada pela criação da Lei em questão, tendo em vista que foi a partir da mesma que houve o nascimento, por via jurisprudencial, do direito fundamental à confidencialidade e integridade dos sistemas informáticos.

## 5. A crescente necessidade de ocultação da investigação criminal

Nas últimas décadas a criminalidade sofreu grandes mudanças, onde a evolução da criminalidade organizada e violenta juntou-se com a crescente ameaça do terrorismo, do fenômeno da globalização, e com a disseminação de novas tecnologias capazes de fomentar a prática de ilícitos e a reduzir a possibilidade de detecção dos mesmos. Assim, aumentou-se a sensação de insegurança, gerada pelos novos riscos da pós-modernidade e agravada pelo sucesso de ataques terroristas em grandes capitais do mundo, levando a sociedade a tolerar a imposição de medidas progressivamente mais

[193] ANDRADE, Manuel da Costa. 2009, p. 166-169.
[194] Conforme informações contidas no site: http://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php. E também:https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html. Acesso em: 04/01/2018.

restritivas de direitos fundamentais, como a privacidade e liberdade, sob o pretexto da recuperação da segurança por parte do Estado. A preocupação é legitima, e o estado de vigilância que ela induz é, até certo ponto, necessário. Todavia, como já tratado aqui, deve existir uma conciliação entre a consagração de mecanismos processuais que permitam uma legítima e eficaz perseguição penal com o respeito dos direitos e garantias de defesa dos cidadãos por eles visados. Assim, tanto a eficácia como a tutela dos direitos e garantias pressupõem a adequação dos meios processualmente existentes ao objeto e característica do processo.[195]

Sobre isso, Ramalho expõe que:

> "tanto a noção de eficácia, como a de tutela de direitos e garantias dos cidadãos, pressupõem a adequação dos meios processualmente existentes ao objecto e características do processo. No primeiro caso, requer-se, em abstracto, que os meios sejam aptos a identificar o autor do ilícito e a recolher prova processualmente válida para a sua condenação. No segundo caso, requer-se que, em concreto, o sacrifício dos direitos do arguido e a redução das suas garantias sejam os estritamente necessários e constitucionalmente admissíveis para a investigação e obtenção de prova, à luz do critério da proporcionalidade."[196]

Dessa forma, quando a especial gravidade dos ilícitos criminais e a maneira como são executados revelem a insuficiência dos existentes meios para lhe enfrentarem, justifica-se a consagração de novos métodos de investigação e obtenção de prova também mais gravosos e sofisticados. Assim, diferentemente da criminalidade em geral, para a grande e nova criminalidade, ou seja, para o terrorismo e criminalidade organizada, onde as vítimas tem um direito indeclinável a uma proteção reforçada, justifica-se a intensificação do intervencionismo estadual.[197] Mas isso não significa abrir mão de certos limites inultrapassáveis, como o núcleo irredutível da dignidade humana que a todos pertence, e também, nas palavras de Jorge de Figueiredo Dias, a:

> "exigência jurídico-constitucional de não diminuição, pela legislação ordinária e pela sua aplicação, da extensão e do alcance do *conteúdo essencial* dos preceitos constitucionais em matéria de direitos, liberdade e garantias e, portanto também daqueles que pertencem à chamada Constituição processual penal"[198].

[195] RAMALHO, David Silva, 2017, p. 202-204.
[196] *Idem,* p. 204.
[197] *Ibidem.*
[198] DIAS, Jorge de Figueiredo. 2009, p. 812-813.

É nesse sentido que é possível afirmar que o processo penal evolui para poder combater novas realidades de crimes, mas no momento em que essa evolução provoca uma ingerência em direitos fundamentais, a utilização de novos mecanismos de investigação e obtenção de prova não pode ser simplesmente utilizada sem critérios, sob pena de serem usados informalmente pelos órgãos de polícia criminal ou criados e sancionados pela jurisprudência, com a consequência de a falta de legalidade e segurança violar desmedidamente os direitos fundamentais dos visados. Contudo, a evolução do CPP Português não sofreu alterações significativas na matéria de métodos de investigação e obtenção de prova, de modo que as principais mudanças surgiram a partir de diplomas extravagantes com regimes processuais distintos para tipos de criminalidade específicos, onde a falta de sistematicidade e de referencial valorativo tornam aparentemente aleatórios o objeto e âmbito de aplicação desses novos meios processuais extravagantes.[199]

Sobre essas novações legislativas, Costa Andrade entende que todas acabam tendo o mesmo resultado final:

> "a redução e neutralização de garantias de defesa; multiplicação, em número e potencial de lesividade e devassa, dos meios institucionalizados de intromissão nos direitos fundamentais; deslocação das linhas de equilíbrio normativo do lado da liberdade, da autonomia e da dignidade, para o lado da segurança (...)"[200].

Entre essas novações, sofrendo deficiências pelo "descaso" do legislador, está o limitado catálogo de métodos ocultos de investigação, que vão surgindo conforme os novos tipos de criminalidade fazem ser necessários, sem uma unidade sistemática de como devem ser utilizados pelo aplicador do direito. Assim, foi surgindo novos métodos ocultos de investigação criminal no ordenamento jurídico Português, como o agente encoberto, previsto no regime jurídico das ações encobertas para fins de prevenção e investigação criminal, aprovado pela Lei nº 101/2001, de 25 de agosto; as medidas de combate á criminalidade organizada, previstas na Lei nº 5/2002, de 11 de janeiro, em particular o registro de voz e imagem, previsto no artigo 6º; ou, mais recentemente, os métodos ocultos de investigação previstos na Lei nº 109/2009, de 15 de setembro.

[199] RAMALHO, David Silva, 2017, p. 205-206.
[200] ANDRADE, Manuel da Costa, Métodos ocultos de investigação (Pladoyer para uma teoria geral), in: Gelson Bonato (org.) Processo Penal, Constituição e Crítica - Estudos em homenagem ao Prof. Dr. Jacinto Nelson de Miranda Coutinho, Rio de Janeiro: Lumen Juris, 2011, p. 528.

Segundo Hans-Jorg Albrecht, estes métodos ocultos tem em comum pelo menos quatro características não necessariamente cumulativas: 1) são ocultados do visado e neutralizam alguns dos seus direitos processuais convencionais, principalmente o direito á não autoincriminação; 2) são abrangentes, na medida em que incidem sobre um número elevado de terceiros e permitem recolher informações que atravessam o passado, presente e futuro e não se limitam ao período relativo aos fatos sob investigação; 3) neutralizam igualmente o direito de certas testemunhas não prestarem declarações; 4) e permitem recolher informações sem ter em atenção a intimidade e fiabilidade da comunicação.[201]

É em razão de tais características e dos variados direitos fundamentais que atingem, como demonstrado anteriormente, que os métodos ocultos tem primordialmente um caráter excepcional, e mesmo nos casos da mais grave criminalidade, não automático, de modo que sua utilização em qualquer investigação criminal sempre implica uma ponderação da sua proporcionalidade, devendo seguir determinados princípios que serão analisados posteriormente.

Ocorre que, apesar da sua elevada danosidade social e da subtração de diversos direitos fundamentais, os métodos ocultos se tornaram essências para investigação de determinados crimes, sobretudo os cometidos em ambiente digital, não podendo se abrir mão de tais mecanismos quando a gravidade do caso assim o justifique.

[201] ALBRECHT, Hans-Jorg. *"Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos*, em AA.VV, Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português, Coimbra: Coimbra Editora, 2009, p. 726.

# IV. AÇÕES ENCOBERTAS EM AMBIENTE DIGITAL

Em 1994 o FBI iniciou uma investigação visando detectar a prática de ilícitos relacionados com pornografia infantil na Internet. Assim, o agente do FBI, D. Douglas Rehman, participou, a partir de Orlando na Flórida, de uma ação encoberta em salas de *chat* criadas por utilizadores do serviço AOL, onde o mesmo se fazia passar por um pedófilo autointitulado de "Mikey1L". O foco da investigação eram as salas de *chat* com temas "*Boys"* e "*Preteen",* as quais eram frequentadas por utilizadores interessados em trocar arquivos com material pornográfico-infantil.[202]

Enquanto frequentava as salas de *chat* o agente Rehman gravava todas as conversas nelas existentes, sem delas participar, permanecendo como um espectador. Em certas ocasiões, diferentes utilizadores enviavam e-mails com arquivos com conteúdo de pornografia infantil para uma lista composta pelos participantes habituais do *chat*, na qual constava o agente do FBI. Um desses utilizadores que enviou e-mails utilizava o nome "Charbyq", que posteriormente foi identificado como Kenneth Charbonneau, residente em Dublin, Ohio. A partir da realização de buscas, o FBI encontrou na casa do mesmo, arquivos informáticos da referida natureza, o que resultou na acusação de Charbonneau por distribuição de pornografia infantil.[203]

Perante o Tribunal Distrital de Ohio, Charbonneau veio a pedir, entre vários outros pedidos, a inadmissão como prova (*motion to suppress evidente*) das declarações por ele proferidas nas salas de *chat* e dos e-mails por ele enviados com arquivos de pornografia infantil, sob a alegação de que os mesmos foram recolhidos em violação aos seus direitos previstos na Primeira e Quarta Adendas à Constituição dos EUA, ou seja, em violação ao seu direito de liberdade de expressão e a uma expectativa razoável de privacidade, respectivamente. Da análise dos pedidos, o Tribunal repudiou liminarmente o primeiro, referindo que o suspeito não tinha se baseado em qualquer jurisprudência, e que a extensão do direito à liberdade de expressão não abrange a transmissão de pornografia infantil. Quanto ao segundo argumento, concluiu pela sua improcedência com base em uma analogia entre, por um lado, o envio de e-mails e o envio de cartas, e, por outro, o envio de mensagens numa sala de *chat* e a comunicação em uma sala física na qual estão presentes várias pessoas.[204]

[202] RAMALHO, David Silva, 2017, p. 281.
[203] *Ibidem.*
[204] *Idem*, p. 282.

No que se refere ao envio de e-mails, o Tribunal sustentou que no caso em questão seria aplicável o entendimento prévio do Tribunal em matéria de correspondência, onde apenas existe expectativa razoável de privacidade entre o momento em que o envelope é fechado e aquele em que a carta chega ás mãos do destinatário, mas não mais após a recepção da comunicação pelo destinatário, ainda que este, por engano propositalmente provocado, seja um agente encoberto do FBI. Por fim, o Tribunal de Ohio concluiu que as declarações de Charbonneau não se encontravam abrangidas pela tutela constitucionalmente garantida ao direito à privacidade, tendo em vista que a participação em salas de *chat*, assim como as conversas em locais públicos, implica a possibilidade de estar presente um agente encoberto que possa ler, ouvir e utilizar as declarações para perseguição criminal do seu autor.[205]

Esse caso citado pelo autor referência do presente trabalho, demonstra claramente a tendência global de não distinguir as ações encobertas em ambiente físico das que ocorrem em ambiente digital. Tendência essa que ocorre principalmente pela escassez de base legal específica dedicada ás ações encobertas em ambiente digital, compensada pela aplicação direta do regime geral a ambas as realidades.[206]

Contudo, antes de analisarmos quais consequências práticas essa aplicação implica, devemos referir sobre dois métodos de obtenção de prova em ambiente digital previstos da Lei do Cibercrime de Portugal, e que ainda que não sejam considerados como ocultos, merecem referência no presente estudo, tendo em vista sua importância.

### 1. O acesso a dados informáticos armazenados, na Lei do Cibercrime de Portugal

O art. 14º da Lei do Cibercrime (109/2009), prevê a injunção para apresentação ou concessão do acesso a dados, onde no seu nº 1 refere:

> "se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência."

[205] *Ibidem.*
[206] *Idem*, p. 283.

Ainda que este meio de obtenção de prova não seja necessariamente oculto, já que constará imediatamente nos autos em processos não sujeitos a segredo de justiça e poderá ser do conhecimento do visado, isso não obsta, conforme entendimento de Mesquista, que seja efetivamente ocultado, seja para identificação do suspeito da prática do fato, ou quando assim se mostra mais adequado aos interesses da investigação.[207]

A injunção para apresentação ou concessão do acesso a dados é aplicada, geralmente, com respeito ao nº 4 do mesmo artigo, que prevê a sua aplicação frente a fornecedores de serviço de modo a que estes comuniquem ao processo dados relativos aos seus clientes ou assinantes, incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma e que permita determinar: i) o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; ii) a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou iii) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.[208]

Importante mencionar também o nº 6 do referido art. 14°, que prevê que não pode fazer-se uso da injunção quanto a sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista, visando manter-se assim, o sigilo profissional.

Contudo, a problemática do artigo em análise decorre da possibilidade de se ordenar a entrega de dados armazenados em território estrangeiro. Essa questão ocorre com frequência nos casos de serviços de computação em nuvem, onde muitas vezes é impossível ou muito difícil saber onde estão armazenados os dados informáticos, e

---

[207] MESQUITA, Paulo Dá. "*Prolegómeno sobre prova electrónica e interceptação de telecomunicações do Direito Processual Penal português – o Código e a Lei do Cibercrime",* em Processo Penal, Prova e Sistema Judiciário, Coimbra: Coimbra Editora, 2010, p. 113, apud RAMALHO, David Silva, 2017, p. 267.

[208] *Ibidem.* Sobre a matéria, refere-se o Acórdão do Tribunal da Relação de Lisboa, processo nº 1695/09.5PJLSB.L1-9, tendo a seguinte ementa: "*I. estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respectiva obtenção é do M°P° II. a identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa III. os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais*." Ainda, na mesma decisão foi entendido que o fornecimento de dados dessa natureza não corresponde á interceptação de comunicações privadas.

enquanto se aguarda a confirmação da localização dos mesmos, pode o seu titular eliminá-los. A Convenção Europeia sobre Cibercrime (Budapeste, 23/11/01), parece oferecer uma luz sob essa problemática, admitindo o acesso remoto e transfronteiriço a dados informáticos, desde que a pessoa a quem a injunção é dirigida esteja em território nacional e tenha a disponibilidade ou controle legal dos dados em causa (conforme estabelece o art. 18, nº 1, alínea *a* da Convenção). Ou seja, o único critério de conexão territorial com os dados que a Convenção exige é a presença da pessoa que tem a disponibilidade ou controle dos dados no território onde se encontra a autoridade que lhe dirige a injunção.[209]

Mas outras dificuldades de ordem prática surgem também na matéria de injunção, como, por exemplo, quando se pretende dirigir a mesma a fornecedores de serviços de computação em nuvem que funcionam de forma integrada e por camadas (como a Dropbox, que se baseia no serviço de infraestrutura da Amazon). A dificuldade ocorre também nos casos em que a entidade notificada guarda os dados cifrados e não dispõe da possibilidade de os decifrar sem a chave de acesso do utilizador, o que vem sendo adotado cada vez mais em razão dos acontecimentos recentes que aumentam a preocupação com a privacidade.[210]

O outro artigo da Lei do Cibercrime que merece destaque aqui é o da pesquisa de dados informáticos, art. 15º, o qual foi previsto pelo legislador através da adaptação ao ambiente digital do regime das buscas em ambiente físico. Assim, previu nos números 1 a 4 do artigo 15º uma regulação praticamente idêntica á prevista no art. 174º, nº 2 a 6, do CPP, remetendo a regulação da sua execução, com as necessárias adaptações, ás regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista (nº 6 do art. 15).

A maior inovação foi através do nº 5 do artigo em questão, que prevê que:

> "quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2."

Com isso, foi consagrado o acesso remoto, e possivelmente transfronteiriço, a dados informáticos armazenados em sistemas informáticos acessíveis através do sistema

[209] RAMALHO, David Silva, 2017, p. 270-271.
[210] *Idem*, p. 271.

inicialmente pesquisado, como ocorre com sistemas de computação em nuvem. Porém, tal diligência não poderá ser oculta, de modo que como decorre do texto da norma, a pesquisa ao sistema informático acessível á distância deverá partir de uma pesquisa informática inicial diretamente no sistema pesquisado, realizada com a presença da autoridade judiciária e, como tal, tendencialmente na presença ou com o conhecimento do suspeito, pelo menos quando seja o proprietário, possuidor ou utilizador frequente do sistema informático inicial.[211]

Em suma, tendo em vista que por não ser considerado um método oculto não iremos trata-lo de maneira exaustiva, pode-se dizer que a norma do art. 15, nº 5, trata-se de uma extensão do nº 1 do mesmo artigo, onde se tem primeiramente o acesso remoto premeditado a um sistema informático e baseado em um mandado especificamente direcionado á recolha de dados nele armazenados, e posteriormente, caso necessário, a pesquisa será estendida a um outro sistema informático ou a outra parte do sistema pesquisado, desde que esses novos dados pesquisados sejam legitimamente acessíveis a partir do sistema inicial.[212]

## 2. O agente encoberto e os seus desdobramentos em ambiente físico e digital

Feitas tais considerações, cabe-nos adentrar na análise feita por Ramalho, do agente encoberto em ambiente digital, que como já referido, por na maioria dos ordenamentos jurídicos não existir uma previsão legal especifica de tal modalidade, acaba por ser aplicado o regime previsto para o agente encoberto no mundo físico. Mas a opção por essa aplicação, ainda que não seja o ideal, não mostra grandes problemas no plano da eficácia e da legitimação constitucional, desde que conjugada com certa liberdade operacional e tendo em vista que grande parte da informação obtida na Internet é informal ou a partir de fontes publicamente acessíveis. Assim, a ação encoberta em ambiente digital é vista como uma modalidade ou outra vertente da ação encoberta, e não como um novo método de investigação criminal, a conjugar frequentemente com a recolha de informação a partir de fontes abertas, e, como tal é entendida – incorretamente – como integralmente subsumível ao regime geral.[213]

[211] *Idem*, p. 272.
[212] *Ibidem.*
[213] *Idem*, p. 283-284.

O denominador comum de ambas as modalidades de ações encobertas, tornando juridicamente possível a aplicação do mesmo regime, é a ocultação ativa ou passiva da verdadeira identidade do agente, somada com a interação com terceiros por meio da identidade fictícia, buscando conquistar a confiança desses terceiros para mais facilmente recolher a prova incriminatória. Contudo, ainda que a essência seja a mesma, onde ambas as modalidades tem em comum os citados aspectos fundamentais, cremos que há necessidade de regulamentação adicional. Encaixar uma realidade complexa a outra realidade simples e com diferenças relevantes, tratando-se de mundos distintos (físico e digital), poderá revelar insuficiências em certos casos específicos, gerando uma margem de liberdade operacional muito ampla capaz de provocar soluções casuísticas, potencialmente inseguras e inadequadas.[214]

Uma das diferenças operacionais que a ação encoberta em ambiente digital demonstra, é a possibilidade de um agente encoberto assumir diversas *personalidades* ao mesmo tempo, em diferentes *espaços virtuais,* e até mesmo com a mesma *aparência* de alguém conhecido da organização que se pretende infiltrar. Por exemplo, o agente encoberto em ambiente digital pode participar em varias salas de *chat* ao mesmo tempo sob identidades diferentes na mesma sala ou em salas distintas, onde em uma pode ser o pedófilo e na outro um menor de idade, ou em uma ser o traficante e em outra o comprador de droga; ou ainda, pode adotar a identidade virtual de outra pessoa próxima do visado, utilizando-se da conta de usuário do mesmo. Ainda, o agente encoberto em ambiente digital corre menos riscos do que o agente em ambiente físico, o que acentua a diferença entre ambos, onde no primeiro caso o agente pode realizar a atividade investigativa no conforto do seu gabinete ou até mesmo do seu lar, não necessitando expor sua imagem física, podendo interagir com suspeitos de várias partes do mundo e em varias salas de *chat* ou *websites* voltados para o crime, integrando-se em grupos organizados com o único interesse em comum de praticar ilícitos, e, principalmente, pode falhar sem que isso traga graves consequências para sua segurança.[215]

Porém, devemos ter em mente que essa segurança adicional aliada com o conhecimento técnico que o agente encoberta deverá ter, proporcionará ao mesmo uma liberdade de aproveitar-se do acesso privilegiado a diversas *personalidades virtuais* e das tecnologias a sua disposição para benefício próprio, praticando ilícitos não relacionados com a ação encoberta ou tirando proveito do próprio ilícito em

[214] *Idem*, p. 284.
[215] *Idem*, p. 284-285.

investigação, praticando crimes com uma identidade e recolhendo prova com outra (como exposto no caso *Silk road* tratado inicialmente, onde dois agentes se aproveitaram das suas condições perante a investigação apropriando-se de centenas de milhares de dólares em *bitcoin*). É nesse sentido que o elevado poder do agente encoberto em ambiente digital implica um dever acrescido de controle por parte da autoridade judiciária e uma obrigação de registro constante de toda atividade praticada pelo agente.[216]

Por outro lado, se faz de suma importância tratar também sobre a controvérsia diante da consagração do agente encoberto entre os métodos ocultos de investigação na lei portuguesa, tendo em vista que tal figura jurídica omite dolosamente a sua identidade com o intuito de capturar outrem na pratica de um ilícito, gerando questões delicadas em matéria de lealdade processual e da superioridade do Estado diante do suspeito. Pode-se dizer que o que implica na utilização de tal figura por parte do Estado é a ineficiência do mesmo no desempenho das suas funções de tutela da segurança, buscando a reafirmação do Direito por um meio que marca o início da conversão do *sujeito investigado* em *objeto* no processo penal. É em razão disso que a decisão admitindo tal método deve ser dada com extrema cautela e a título excepcional. Nesse sentido, a justificativa constitucional da ação encoberta deve se dar através dos fins por ela prosseguidos, em razão dos direitos e interesses por ela sacrificados, devendo as restrições de direitos, liberdades e garantias limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos (conforme nos ensina o art. 18, nº 2, da Constituição da República Portuguesa).[217]

Assim, Franklim Furtado, ao referir sobre a legitimação do agente encoberto, destaca que

> "a eficácia no combate torna-se assim essencial e não será impróprio dizer-se que ela ganha uma dimensão ética, porquanto se ela falecer ou for insuficiente, a sociedade ver-se-á desamparada face ao crime e aos criminosos e o Estado verá frustrado seus fins mais elementares."[218]

Portanto, ainda que a utilização de agentes encobertos demonstre certos perigos e deslealdade, é impossível renunciar ao serviço do *undercover agent* quando se está em

[216] *Idem*, p. 286.
[217] PEREIRA, Rui. O "agente encoberto" na ordem jurídica portuguesa, em AA.VV., *Medidas de combate á Criminalidade Organizada e Economico-Financeira*, Coimbra: Coimbra Editora, 2004, p. 18-19, apud RAMALHO, David Silva. 2017, p. 288.
[218] FURTADO, Franklim. "*O agente infiltrado"*, Direito e Cidadania, Ano V, nº 16/17 (setembro de 2002/abril de 2003), p. 9.

causa certo tipo de criminalidade grave (terrorismo, tráfico de droga, criminalidade violenta ou organizada). Assim, deve-se aceitar aqui uma excepcionalidade no modo de obter as provas tendo em vista os interesses que se entrecruzam e os meios tão sofisticados que os criminosos dispõem.[219]

Contudo, é importante destacar que o fato de um órgão de polícia não se identificar não implicará sempre e automaticamente na aplicação do regime encoberto e nas considerações feitas acima, pois caso fosse de tal maneira, a simples presença de um agente não fardado em qualquer local poderia significar uma ação encoberta. Assim, na definição da doutrina de Manuel Alves Meireis, agente encoberto é

> "um agente da autoridade, ou alguém que com ele actua de forma concertada, que sem revelar a sua identidade ou qualidade, frequenta os meios conotados com o crime na esperança de descobrir possíveis delinquentes; não provoca ao crime, nem conquista a confiança de ninguém"[220].

Ou seja, sob essa definição, pode ser um comum agente *á paisana*, tratando-se de um meio de obtenção de prova atípico e não proibido por lei, encontrando-se abrangido pelo disposto no art. 125 do CPP. Ocorre que entendemos[221] que a definição exposta acima se mostra insuficiente, uma vez que excluiria das ações encobertas os casos em que o agente policial se imiscui no contexto onde ocorrem as atividades criminosas e interage com os suspeitos, estabelecendo, consequentemente, laços de confiança, tudo com o intuito de prevenir a prática de ilícitos e obter informações da atividade criminosa e/ou recolher provas incriminatórias, mas sempre abstendo-se de provocar a prática de quaisquer ilícitos[222]. Essa seria a definição de agente infiltrado, que para nós, se confunde com o agente encoberto, tratando-se da mesma figura, prevista na Lei 101/2001 (ações encobertas).

Porém, o que não pode ser confundido, merecendo a devida distinção, é o agente encoberto/infiltrado do agente provocador. A principal distinção entre ambas as figuras é que no segundo caso o agente provoca uma intenção, até então inexistente, de outrem praticar um ilícito. Em síntese, o agente provocador é o órgão de polícia

---

[219] Conforme Acórdão TC, de 14/10/1998, Processo nº 835/98, Relator Messias Bento, disponível em www.tribunalconstitucional.pt.

[220] MEIREIS, Manuel Alves. O regime das Provas Obtidas pelo Agente Provocador em Processo Penal, Coimbra: Almedina, 1999, p. 192-193.

[221] Conforme RAMALHO, David Silva, 2017, p. 289-290.

[222] SOUSA, Susana Aires de. "*Agent provocateur e meios enganosos de prova. Algumas reflexões",* em AA.VV, Liberdiscipulorum para Jorge de Figueiredo Dias (org. Manuel da Costa Andrade *et al.),* Coimbra: Coimbra Editora, 2003, p. 1222.

criminal ou um terceiro sob a sua direção que estimula outrem a cometer um crime que de outro modo não seria praticado, geralmente motivando-se na facilidade de recolher a prova do fato criminoso.[223]

Para Germano Marques da Silva, a provocação não é apenas informativa, mas sobretudo formativa, não revelando o crime e o criminoso, mas sim criando-os. Assim, essa provocação acaba alterando a finalidade do processo penal (realizar a justiça através da perseguição criminal dos culpados), pois cria o crime que visa punir, transformando o inocente em culpado.[224] Portanto, entende-se que o agente provocador viola os princípios da democracia e da lealdade, assim como do processo justo e equitativo, maculando esse meio de obtenção de prova enganoso e não legitimado com a nulidade das provas obtidas com tal ofensa da integridade moral do visado, com força no previsto nos artigos 32, nº 8, da CRP, e 126, nº 2, alínea *a)*, do CPP.[225]

Feita tal distinção, deve-se trazer também aqui os três elementos fundamentais que compõem o agente encoberto e que tornam sua utilização particularmente grave. Como primeiro e principal elemento, Ramalho cita a já referida ocultação da qualidade e identidade do agente no meio onde se infiltra, tratando-se de uma verdadeira conduta ativa de encobrimento da identidade e, caso necessário, de mentira quanto a mesma. O segundo elemento destacado pelo autor, jaz no ato de infiltração, onde o agente integra-se no meio criminoso de forma passiva ou ativa (tentando ganhar a confiança dos suspeitos). Por fim, o terceiro elemento é o da necessidade da ação encoberta recolher a prova da intenção da pratica de crimes ou do seu efetivo cometimento. Portanto, o agente oculta sua identidade, infiltra-se no meio criminoso e recolhe a prova que levará a responsabilidade criminal dos visados, podendo até mesmo prevenir a prática de outros ilícitos.[226]

Implícito a esses elementos está um conjunto de regras sociais e comportamentais que o agente deve seguir para que obtenha sucesso na sua missão de se infiltrar no mundo do crime sem ser descoberto e assim ganhar a confiança daqueles que visa punir, para, finalmente, obter a prova incriminatória que de outro modo seria muito difícil ou impossível de recolher.[227]

---

[223] RAMALHO, David Silva. 2017, p. 291. No mesmo sentido: ANDRADE, Manuel da Costa. 2011, p. 537.
[224] SILVA, Germano Marques da. *Bufos, infiltrados, provocadores e arrependidos,* in Direito e Justiça, F.D.U. Católica, vol VIII, T. 2, 1994, p. 29.
[225] SOUSA, Susana Aires de. 2003, p. 1231-1235.
[226] RAMALHO, David Silva. 2017, p. 292-293.
[227] *Idem,* p. 293.

Ocorre que a interação social na Internet difere muito da interação em ambiente físico, já que nela, diferentemente do que ocorre no ambiente físico, e em particular através de fóruns, *chats*, ou outros *websites*, a ocultação da identidade é a regra perante todos, sendo a identificação pessoal a exceção. Os cibernautas se identificam e interagem com os outros através de *usernames* ou *nicknames*, independentemente da atividade que estão desempenhando na rede, exceto quando a identificação pessoal seja proposital, como ocorre nas redes sociais. As pessoas se comunicam entre si sem saber a identidade, aparência física ou até mesmo o país da outra, não necessitando o agente policial de grandes esforços para esconder sua real identidade. Outro fator aqui, é que há uma enorme quantidade de informação com relevo probatório disponível online onde a sua recolha não necessita de qualquer interação com os suspeitos, restando apenas no aguardo da sua obtenção. Basta recordar dos casos expostos anteriormente do *United States vs. Ross Ulbricht* ou no caso *United States vs. Charbonneau*, onde as informações recolhidas pelos agentes que criaram contas de utilizador para fins investigativos estavam livremente acessíveis, tendo em vista que no primeiro caso havia ofertas de venda de material ilícito no *website Silk road*, e no segundo houve o envio de ficheiros com pornografia infantil para os participantes de um *chat*. Portanto, a atividade criminosa nesses casos ocorre às claras, o que é difícil mesmo e justifica o recurso às ações encobertas em ambiente digital é a imputação das condutas aos seus reais autores.[228]

Nesses casos onde há interação pública em *chats*, fóruns e *websites*, acessíveis por meio de um simples registro prévio e geralmente não controlado, se observa uma configuração totalmente diversa dos elementos expostos anteriormente que compõem o agente encoberto. Quanto ao primeiro elemento, a ocultação da real identidade do agente, verifica-se como uma consequencia do ambiente em que se insere, já que todos se identificam com nomes fictícios, como já referido. Da mesma forma o segundo elemento, a infiltração, não mostra qualquer dificuldade, já que o acesso ao grupo é concedido com o mero registro de usuário. E o terceiro elemento, a recolha de prova incriminatória, também se encontra livremente disponível. Ou seja, onde a identificação entre os participantes se dá apenas através de *usernames*, onde há uma global ausência de confiança e uma geral partilha de informação e documentos de interesse comum, basta ao agente entrar nos grupos e assistir livremente o que se passa, recolhendo as

[228] *Idem*, p. 293-294.

provas dos ilícitos em questão. Vale destacar a observação de Ramalho, quando o autor destaca que dificilmente poderia se fazer uma analogia de uma situação dessas no mundo físico, pois em um espaço físico destinado a pornografia infantil ou vendas de drogas e armas, não seria concebível que um terceiro pudesse entrar sem se identificar e assistir á tudo que ocorre.[229]

É em razão dessas questões expostas que levanta-se o questionamento se em tais casos poderia considerar-se a ocorrência de uma ação encoberta, parecendo-nos que o simples acesso passivo e inócuo do agente em *websites* e *chats* pode ser admissível fora do contexto de ações encobertas.[230] Segundo a doutrina espanhola, tal pratica trata-se do que se chama de *ciberpatrullaje*, representando um momento prévio às ações encobertas, realizadas por um agente com o fim aleatório de imiscuir-se em fóruns e comunidades para ver o que lá ocorre ou para ver se descobre algum delito por casualidade.[231]

Por outro lado, e se supormos que o agente se apresente perante os demais participantes do *chat online* onde é sabido a presença frequente de pedófilos com o *username 12yearsoldgirl*? Ou em um *chat* voltado para o tráfico de drogas e usar o nome *ineedmarijuana*? Ou ainda, usar o nome de um antigo participante do grupo criminoso que já foi capturado pela polícia e revelado suas respectivas credencias? Tais atitudes por parte do agente encoberto podem ser consideradas uma comunicação e solicitação de contato para a prática de ilícitos, porventura provocadora. E mais. E se o agente encoberto decidir participar da comunicação e falar no *chat* ou comentar algo no *website* escondendo sua real identidade? A sua conduta ativa, interagindo com os demais e passando a assumir um contato privado com indivíduos determinados (através do uso de janelas privadas de conversação, e-mails ou outras formas de comunicação via Internet) somado com a ocultação da sua identidade, revela, de acordo com Ramalho, uma potencial danosidade social, estando esses casos sem dúvida alguma no contexto das ações encobertas e, consequentemente, dos métodos ocultos de investigação criminal.[232]

Nessas situações, o agente pode estabelecer comunicações com indivíduos cuja real identidade desconhece mas que pretende descobrir, ou também pode iniciar o

[229] *Ibidem.*
[230] *Idem*, p. 297.
[231] NUÑEZ, Eloy Velasco. *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid: La Ley, 2010, p. 212.
[232] RAMALHO, David Silva, 2017, p. 296.

contato por conhecer a identidade física e virtual do visado, visando a obtenção de provas contra o mesmo ou maiores informações da organização criminosa a que eventualmente venha pertencer, e inclusive vir a participar das comunicações entre os membros da organização, o que irá requerer, é claro, uma maior infiltração e dissimulação por parte do agente. Independente do caso, o que é imprescindível é que toda essa operação investigativa siga os requisitos e princípios dos quais depende uma ação encoberta legitima, para não macular as provas obtidas com uma insanável nulidade.[233]

### 3. A Lei nº 101/2001 e o agente encoberto em ambiente digital

No ordenamento jurídico português, a Lei nº 101/2001, de 25 de agosto, estabelece o regime das ações encobertas para fins de prevenção e investigação criminal, considerando-se, segundo seu art. 1º, nº 2, ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controle da Polícia Judiciária para prevenção ou repressão dos crimes indicados no art. 2º da Lei, com ocultação da sua qualidade e identidade.

Contudo, há diversos aspectos criticáveis na Lei em questão, tornando duvidosa a constitucionalidade de várias das suas disposições. Uma das criticas é o fato de não cumprir o princípio da reserva de juiz, tendo em vista que para a admissibilidade e inicio da ação encoberta basta o mero silencio da autoridade judicial perante a iniciativa do Ministério Público (art. 3º, nº 3), exceto se a medida for visada para fins de prevenção criminal, onde então será necessária a previa autorização do juiz de instrução criminal, mediante proposta do Ministério Público (art. 3º, nº 4). Prevista de tal forma, a norma não oferece garantias de proporcionalidade na sua aplicação e não oferece qualquer tutela preventiva aos direitos fundamentais do visado, bem como não permite encontrar uma fundamentação judicial para a respectiva sindicância.[234] Nas palavras de David Silva Ramalho:

> "está em causa, não um acto judicial, que sempre deveria ser devidamente fundamentado (cf. artigo 97º, nº 3, do CPP e 205º, nº 1, da CRP), mas sim uma omissão judicial constitutiva da validade da acçao encoberta, que frustra a finalidade da exigência geral de reserva de juiz."[235]

[233] *Ibidem.*
[234] *Idem,* p. 302.
[235] *Ibidem.*

Somado a isso, está a falta de qualquer norma que regule a conduta do agente encoberto (como os atos a empreender), bem como a omissão de previsão de um prazo máximo para duração da medida e o fato de não existir obrigação legal de revisão dos seus pressupostos. Nessa linha, a validação da medida por um juiz envolveria a elaboração de um plano de ação indicando de uma maneira geral quais os atos autorizados ou não ao agente e o tempo de duração da ação.[236]

Ademais, se mostrando como o elemento que talvez mais fere as garantias de defesa do arguido, impossibilitando uma ampla defesa e um contraditória digno, é o fato de que o relato do agente encoberto será, em regra, colocado fora dos autos, de modo que nem o arguido e nem o juiz de julgamento terão conhecimento e acesso á ele, a não ser que a autoridade judiciária entenda que o mesmo poderá ter relevo probatório (para a acusação). Essa exigência visa manter a segurança do agente encoberto, tendo em vista que se o acusado tiver acesso ás declarações do agente, poderá descobrir sua identidade, colocando o mesmo em risco. Contudo, essa não deveria ser a regra, mas sim a exceção, aplicando-se somente nos casos em que realmente fosse verificado um risco para a segurança do agente.[237]

Já no âmbito digital, o legislador incluiu através da Lei do Cibercime (Lei nº 109/2009, de 15 de setembro), uma norma dedicada especificamente para as ações encobertas em matéria de cibercrime. Estamos falando do art. 19º da Lei, que acrescenta certos crimes informáticos ou cometidos através de um sistema informático ao catálogo previsto no art. 2º da Lei 101/2001, ou seja, permitindo que tais crimes sejam investigados com recurso ao agente encoberto quando assim se mostrar necessário, e recorrendo sempre aos termos previstos na Lei 101/2001. A alínea *b)* do art. 19º da Lei do Cibercrime prevê quais crimes podem recorrer ao uso do agente encoberto em ambiente digital:

> "os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos."

[236] *Ibidem.*
[237] COSTA, Eduardo Maia. "*Ações encobertas (Alguns problemas, algumas sugestões*)", em AA.VV., Estudos em Memória do Conselheiro Artur Maurício, Coimbra: Coimbra editora, 2014, p. 367-368.

Da mencionada norma, constata-se a consagração do agente encoberto em ambiente digital (e, consequentemente, todos os seus desdobramentos referidos anteriormente), mas a partir de uma observação mais profunda da mesma, Ramalho entende que podem ser observados também, os seguintes fatores: a) ao reduzir o seu objeto a cibercrimes muitas vezes de gravidade media ou com penas relativamente baixas, a norma traz implícito um juízo de dificuldade acrescida na obtenção da prova, precisamente decorrente do fato de os ilícitos ocorrerem em ambiente digital; b) levando em conta a finalidade essencialmente preventiva das ações encobertas, se os ilícitos em questão apenas podem ser praticados através de sistemas informáticos, então consequentemente o agente encoberto terá também de estar em ambiente digital para interagir com o suspeito e recolher a prova da prática ou iminência do crime (ao não ser que ocorra a hipótese de o agente estar ao lado do suspeito no momento em que pratica o fato na frente do computador, o que é altamente improvável); c) e, quando for possível recolher a prova fisicamente junto do suspeito ou através de qualquer outro dos meios de obtenção de prova previstos no CPP ou na Lei do Cibercrime, as ações encobertas tenderão a revelar-se desproporcionais (conforme art. 3º, nº 3, da Lei nº 101/2001).[238]

Outro artigo que merece destaque aqui é o art. 6 º, nº 1, da Lei 101/2001, que prevê que:

> "não é punível a conduta do agente encoberto que, no âmbito de uma acção encoberta, consubstancie a prática de actos preparatórios ou de execução de uma infracção em qualquer forma de comparticipação diversa da instigação e da autoria mediata, sempre que guarde a devida proporcionalidade com a finalidade da mesma."

Essa isenção de responsabilidade do agente encoberto levanta duas correntes na doutrina, onde de um lado há quem entenda que é proibida a prática de qualquer ilícito que não seja praticado em comparticipação, exceto se o crime autônomo praticado pelo agente encoberto esteja em uma lógica de comparticipaçao com outro crime, como no caso em que se adquire droga de um traficante para consumo.[239] E de outro lado, há quem afirme que se o êxito da ação encoberta dependa do envolvimento do agente na pratica de crimes, em autoria material (singular), correndo o risco de ser desmascarado, deverá ser admitida sua comissão, desde que preenchido o requisito da necessidade e

[238] RAMALHO, David Silva, 2017, p. 303.
[239] PEREIRA, Rui. "*O "agente encoberto" na ordem jurídica portuguesa*", em AA.VV., Medidas de Combate á Criminalidade Organizada e Econômico-Financeiro, Coimbra: Coimbra Editora, 2004, p. 32.

que não existam ofensas pessoais, com exceção dos casos de legítima defesa e estado de necessidade.[240]

O caminho mais correto parece ser o da cumulação de ambas correntes, admitindo-se a pratica de crimes numa lógica de comparticipação, bem como a prática dos ilícitos que preencherem os requisitos citados acima. Mas e se para a infiltração em um grupo privado *online* depender do envio prévio de um conjunto de arquivos contendo pornografia infantil? Nesse caso, onde o bem jurídico tutelado pertence a um menor, e levando em consideração que o envio de imagens implicará uma perpetuação do dano do crime, não será admissível mesmo que se encontre em uma lógica de comparticipação ou seja condição necessária para infiltração. A única hipótese em que se poderia admitir isso, é se houver o consentimento dos representantes legais do menor ou através de técnicas de anonimização do mesmo. Mas não se pode negar que tal recurso seria muito útil para infectar o sistema informático do suspeito com *malware*, e desse modo recolher a informação pretendida.[241]

[240] COSTA, Eduardo Maia. 2014, p. 365.
[241] RAMALHO, David Silva. 2017, p. 307-308.

# V. O USO DE *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM AMBIENTE DIGITAL

O termo *malware* resulta da contração do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático) e pode ser definido, conforme Boldt, como "um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça"[242] ou, de uma forma mais desenvolvida, como:

> "um programa simples ou auto-replicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático"[243].

Para Ramalho, pode-se dizer que é todo tipo de programa instalado por terceiros em um sistema informático, podendo ser utilizado para, de alguma maneira, comprometer suas funções, contornar os seus controles de acesso, causar prejuízos ao utilizador ou ao sistema informático infetado, monitorar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos.[244]

Entretanto, tais conceitos e ações condizem mais com o *malware* quando utilizado por *hackers* e para fins ilícitos. Quando o programa é utilizado para fins de investigação criminal, estando sob controle de órgãos policiais, o objetivo não é comprometer o funcionamento do sistema informático visado e causar prejuízos ao usuário, corrompendo e eliminando seus dados. Ao invés disso, o *malware* visa aqui "tão somente" invadir o sistema informático (contornando os controles de acesso, como senhas e antivírus) e pesquisar por dados, comunicações, históricos de acesso à Internet, ou monitorar a atividade em tempo real do usuário no seu computador ou em torno dele (caso utilizado o recurso de ativar a *webcam* e o microfone do computador visado, sendo uma espécie de *grande devassa digital* caso o mesmo esteja dentro do domicilio), para que então possam ser encontradas provas que o incriminem pelo crime que está sendo investigado. É nesse sentido que a utilização da expressão malicioso pode causar estranheza, já que estamos falando de um instrumento utilizado por órgãos de polícia

[242] BOLDT, Martin. *Privacy-Invasive Software*, Karlskrona: Blekinge Institute of Technology, 2010, p. 10.Disponível:http://www.bth.se/tek/aps/mbo.nsf/bilagor/boldt_thesis_v1_02_pdf/$file/boldt_thesis_v1.02.pdf. Acesso em: 04/07/2017.
[243] FILIOL, Eric. *Computer viruses: from theory to applications*, França: Springer, 2005, p. 83.
[244] RAMALHO, David Silva, 2017, p. 319.

criminal no contexto de uma investigação, onde o maior objetivo é a realização da Justiça. Entretanto, tal expressão é utilizada sem qualquer carga valorativa em relação à atividade de investigação, mas sim porque se trata de um termo genérico que engloba vários tipos de *malware*, e também por que se trata de um *software* que é intrusivo, insidioso, e assim sendo, malicioso em relação ao sistema informático no qual se instala.[245]

Segundo o autor supracitado, no que diz respeito aos tipos de *malware* existentes, ainda que a maior parte da doutrina mencione apenas os cavalos de Tróia (*Trojans*), existem muitos tipos de *malware* que podem ser utilizados no âmbito de investigações criminais em ambiente digital, como por exemplo, as *logic bombs*, o *spware*, os *rootkits*, os vírus e os *worms*, e as cada vez mais comuns *blended threats* (ameaças mistas), que utilizam mais de um tipo de *malware*. Todavia, no presente trabalho, nos absteremos de conceituar todos os tipos de *malware*, acreditando ser suficiente faze-lo apenas em relação ao mais utilizado, o cavalo de Tróia, tendo em vista que os outros tipos agem de uma maneira semelhante. O cavalo de Tróia se apresenta como sendo inofensivo e induz o visado a executar uma conduta ativa, como um *download* de um anexo de uma mensagem de correio eletrônico ou abrindo uma página *web* infectada com código malicioso, que resultará na instalação do *malware* no sistema informático visado. Ou seja, são os próprios utilizadores que ativam, desavisadamente, as funções nocivas do *malware*, pensando que estão executando um ficheiro ou acessando um *website* inofensivo.[246]

Então, estando o sistema informático infectado, os cavalos de Tróia criam, na maioria das vezes, *backdoors*, entendidos como formas escondidas de acessar remotamente ao sistema, contornando os mecanismos de autenticação existentes. Assim, através desse acesso proporcionado pelo cavalo de Tróia, o terceiro que o instalou pode recolher informações, como credenciais de acesso a páginas reservadas (*webmails*, perfis em redes sociais, etc.), monitorar a atividade do utilizador no sistema infetado, instalar outros tipos de *malware*, ou até mesmo navegar na Internet de forma anônima, enviando informação a partir do computador atacado.[247]

Mas o que deve ser destacado aqui, é que a execução do *malware*, geralmente nos casos dos cavalos de Tróia, inclui uma comunicação a uma entidade controladora

[245] RAMALHO, David Silva, 2013, p. 201.
[246] *Ibidem.*
[247] CRIADO, Miguel Ángel Poveda. *Delitos en la Red: Cibercrimen, Ciberdelitos, Ciberseguridad, Ciberespionaje y Ciberterrorismo*, Madrid: Editora Fragua, 2015, p. 98.

externa (no presente caso, os investigadores) com vista à obtenção de instruções futuras, e dependendo do comando enviado ou do *malware* instalado, pode o controlador remoto registrar as teclas premidas pelo utilizador (por meio de *keyloggers*), acessar seus arquivos e históricos de Internet, vigiar a sua atividade em tempo real, escutar as suas conversas via *Skype* ou outro sistema de *Voice-over-Ip* (VoIP), ou até mesmo permitir ativar a câmara ou o microfone do computador atacado, possibilitando testemunhar diretamente a pratica criminosa. Também podem ser aplicadas certas medidas que permitem ao *malware* permanecer indetectável, substituindo-se por um programa confiável em execução e desativando os programas de antivírus existentes.[248]

Por exemplo, o cavalo de Tróia Back Orifice 2000, que na maioria das vezes era disseminado como anexo em mensagens de correio eletrônico, e permitia ao hacker recolher informações sobre o computador infectado, executar comandos no sistema, redirecionar tráfego da internet e reconfigurar o sistema informático, podendo causar danos inimagináveis no computador e na privacidade da pessoa atingida.[249]

Já no que se refere ao processo de instalação do *malware*, os três principais modelos de infecção são: via suporte físico removível, via *web browser* e via *download* voluntário. Antes da invenção da Internet, a infecção via suporte físico removível era a mais comum, onde na falta de outros meios de propagação, o *malware* espalhava-se por meio de CDs, disquetes ou outros suportes destinados a serem fisicamente conectados a sistemas informáticos. Esse método ainda é utilizado nos dias de hoje, sendo eficaz para atingir redes locais (*Local Area Networks* ou LAN) ou sistemas informáticos desconectados da Internet, e revela particular utilidade na instalação de *malware* para fins de investigação criminal, já que permite que os investigadores se assegurem que apenas o sistema informático visado será infectado, e não vários sistemas indeterminados.[250]

O segundo modelo de instalação de *malware*, como referido, é via *web browser* ou também chamado de *drive-by-download*, em que o utilizador, pensando que está abrindo uma página *Web* inofensiva, acessa uma página composta parcialmente por um código malicioso que detecta vulnerabilidades no sistema informático do utilizador e o

[248] RAMALHO, David Silva, 2013, p. 207.
[249] SINROD, Eric J. e REILLY, William P., *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, Santa Clara Computer and High Technology Law Journal, Vol. 16, nº 2, 2000, p. 223. Disponível em: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1258&context=chtlj. Acesso em: 15/08/2017.
[250] RAMALHO, David Silva, 2013, p. 205.

infecta com *malware*. Outra maneira de instalação existente nesse mesmo modelo é a chamada *malvertising*, que ocorre pelo *download* automático do *malware* quando o utilizador tentar *clicar* em um determinado *link*, geralmente de aspecto publicitário. As potencialidades desse modelo para fins de investigação criminal foram evidenciadas pelo FBI em agosto de 2013, quando implantaram uma forma de *malware* nomeada de *Magneto* nos servidores do *Freedom Hosting*, um fornecedor de serviços que continha inúmeros *hidden services*[251] dedicados à pornografia infantil. Em síntese, o *malware* proporcionava identificar o nome de utilizador do administrador do *Windows* que acessava aos referidos *hidden services*, para posteriormente descobrir também o seu verdadeiro endereço IP e sua localização, permitindo assim retirar o indivíduo da cortina do anonimato e da impunidade pelos atos de pornografia infantil praticados.[252]

Por fim, o *malware* também pode ser instalado em um sistema informático através do *download* voluntário de certos ficheiros, seja através da abertura de certos anexos de correio eletrônico, seja por meio do *download* de programas executáveis (geralmente piratas e gratuitos), ou através de falsas atualizações de *software* legítimo.[253]

## 1. A origem e a evolução do uso de *malware* para fins de investigação criminal: o caso dos Estados Unidos da América

Como é sabido, os Estados Unidos da América (EUA) se mostram sempre como os pioneiros nos mecanismos de vigilância, não podendo ser diferente no que se refere ao uso de *malware* para fins de investigação criminal. Ainda que a experiência norte-americana tenha sido marcada por revelações de usos não autorizados e secretos, e por uma fundamentação jurídica de pouca credibilidade, foi lá onde se passou o primeiro caso de relevância midiática com relação ao uso de *malware* em uma investigação criminal. O caso, objeto de estudo de Ramalho, é relatado abaixo.

Em janeiro de 1999, o FBI investigava um conhecido membro da máfia americana suspeito de infrações relacionadas com gestão de jogos ilegais, Nicodemo S. Scarfo. No âmbito da investigação, com o uso de *keyloggers*, foi descoberto que no

[251] Segundo RAMALHO, 2013, p. 206, "*hidden services* são *websites* acessíveis apenas através do programa Tor (The Onion Router) cujo local de armazenamento é potencialmente indetectável e cujo acesso muito dificilmente permite a identificação dos seus utilizadores".
[252] RAMALHO, David Silva, 2013, p. 206.
[253] *Ibidem.*

computador do investigado existia um conjunto de ficheiros informatizados que se suspeitavam conter elevado valor probatório para o caso. Entretanto, a dificuldade surgiu quando as autoridades se aperceberam que tais ficheiros se encontravam encriptados. Com a intenção de descobrir a *password* que decifraria e permitiria acesso ao conteúdo desses ficheiros, o FBI solicitou novo mandado judicial para uso de um outro *keylogger*, mas que desta vez seria instalado fisicamente e diretamente no computador de Nicodemo. Dois meses após a instalação do *keylogger*, o *password* foi obtido e o conteúdo dos ficheiros foi descoberto, permitindo ao FBI deter o suspeito.[254]

Após a conclusão desse procedimento, as autoridades policiais americanas perceberam a dificuldade para a obtenção de prova em âmbito digital, e em razão da crescente gravidade e internacionalização da criminalidade (principalmente após o 11 de setembro de 2001), tornou-se óbvia a necessidade de uma resposta mais eficaz e de um mecanismo capaz de ser instalado remotamente no computador visado. Dessa maneira, em 2001 o FBI cria o *Magic Lantern*, um *keylogger* que poderia ser instalado remotamente via Internet e através da simples abertura de anexos enviados por *e-mail*, permitindo o conhecimento de todas informações que o visado inseria no teclado, sem que esse tivesse conhecimento que estava sendo monitorado, conforme explicado por Kevin Curran. [255]

Com a evolução tecnológica, o *Magic Lantern* deu lugar ao *Computer and Internet Protocol Address Verifier* (CIPAV), um tipo de *malware* que permitia captar o endereço IP do computador suspeito e a sua localização, o sistema operativo utilizado, os programas instalados e em funcionamento, o último *site* visitado, entre outras funções.[256]

Posteriormente, em abril de 2011, o FBI veio divulgar vários documentos com informações sobre o CIPAV, que possibilitaram concluir que o mesmo era usado com frequência, inclusive por entidades governamentais que não o FBI e para diversas finalidades. As informações também demonstravam a existência de entendimentos divergentes sobre os requisitos legais para a admissibilidade do *malware*, onde de um

[254] *Idem*, p. 213.
[255] CURRAN, Kevin, *et al. Hacking and Eavesdropping,* em *Cyber Warfare and Cyber Terrorism* (orgs. Lech J. Janczewski e Andrew M. Colarik), Nova Iorque: Information Science Reference, 2008, p. 309.
[256] PRADILLO, Juan Carlos Ortiz, *Remote Forensic Software as a Tool for Investigating Cases of Terrorism, ENAC – E-newsletter on the fight againt cybercrime, nº 4,* 2009, p. 3. Disponível em: *http://polis.osce.org/library/f/3643/2779/NGO-ESP-RPT-3643-EN-2779.pdf* . Acesso em: 19/04/2017.

lado estavam os defensores da desnecessidade de qualquer procedimento legal para a sua utilização, e no outro, os defensores da necessidade de autorização judicial.[257]

Segundo a documentação referida, a solução foi pela necessidade de um mandado judicial para a intrusão no sistema informático visado, e posteriormente pela necessidade de uma *Pen/Trap order* para autorizar a vigilância.[258] Nesse sentido, interessante mencionar a ordem judicial de abril de 2013 proferida pelo Juiz Stephen Smith, da Divisão de Houston do Tribunal do Distrito do Texas.[259] Buscava-se autorização para instalar, via e-mail, um *malware* em um computador desconhecido, utilizado por pessoas desconhecidas em uma localização desconhecida. A única informação que existia era que um grupo de pessoas teria obtido acesso ilegal ao e-mail de John Doe, usando o e-mail para acessar a conta bancária do mesmo e praticar fraude. Assim, com o conhecimento que o e-mail ainda era acessado pelos criminosos, o FBI pretendia instalar o *malware* no computador dos mesmos não apenas para acessar dados, mas também para descobrir a sua localização e tirar fotos pela *webcam* dos responsáveis pela operação.[260]

Todavia, ainda que para os investigadores tal ação estaria suficientemente legitimada pela Rule 41, o magistrado entendeu, entre outros fundamentos, que o fato de o computador estar em local desconhecido, tornava a jurisdição incerta, não sabendo se estaria no limite territorial da referida Rule 41. Ainda, ao confrontar o pedido com a quarta Adenda á Constituição norte-americana, o Tribunal entendeu que o *malware* em questão não oferecia garantias de que apenas o mínimo necessário de dados seria recolhido, bem como não era possível garantir que apenas os visados seriam atingidos pela medida, já que os agentes criminosos poderiam utilizar o IP de outrem, ou utilizar o computador de uma biblioteca pública ou de um café, que são locais públicos onde o sistema informático é acessível a varias pessoas. Ainda, o Tribunal entendeu que a ativação da câmera do sistema informático é materialmente uma atividade de vídeo-vigilância, o que requer a verificação de pressupostos adicionais de indispensabilidade, além da imposição de certos limites á sua utilização, como um período máximo da

[257] RAMALHO, David Silva, 2017, p. 326.
[258] Conforme p. 169 da documentação facultada pelo FBI, disponível em https://www.eff.org/files/fbi_cipav-08-p169.pdf. Acesso em: 19/04/2017.
[259] Para maiores informações sobre a decisão, acessar: https://pt.scribd.com/doc/137842124/Texas-Order-Denying-Warrant. Acesso em: 04/08/2017.
[260] RAMALHO, David Silva, 2017, p. 327.

mesma e uma definição dos passos que devem ser adotados para garantir que a vigilância será apenas para os propósitos visados e autorizados.[261]

Contudo, decisões bem fundamentadas como essa não são unânimes, sendo certo que apesar do impacto e das divergências que a medida causou e ainda vem causando, o uso do *malware* persiste no contexto de investigações criminais norte-americanas, não sendo possível precisar se apenas quando há mandado judicial ou mesmo sem ele, em "investigações secretas".

## 2. As buscas online na Alemanha

Assim como nos EUA, na Alemanha o surgimento do *malware* como meio de obtenção de prova causou muitas polêmicas. Como já exposto anteriormente ao analisar a criação jurisprudencial do *direito fundamental à confidencialidade e integridade dos sistemas informáticos,* foi a partir da aprovação da Lei para a defesa face aos perigos do terrorismo internacional, de 25 de dezembro de 2008, que se introduziu expressamente no ordenamento jurídico alemão, de acordo com as exigências do BVerfG, a possibilidade, a título excepcional, da utilização de *malware* (buscas online) para prevenção de crimes de terrorismo.

Ocorre que, no dia 8 de outubro de 2011, uma associação de *hackers* autointitulada de *Chaos Computer Club* (CCC) divulgou (causando grande impacto na comunicação social), uma informação de que parte de órgãos de polícia criminal alemães estavam utilizando um tipo de *malware* (geralmente referido como um cavalo de Tróia, mas aparentemente uma *blended threat*) que viria a ficar conhecido como *Bundes trojaner* ou *Staats trojaner*. O episódio também mereceu análise de Ramalho. Segundo o autor, tratou-se de um *malware* enviado para o computador do suspeito na forma de uma comum atualização de *software*, mas que, depois de instalado, possibilita monitorar toda a atividade do investigado na Internet, como gravar as chamadas de Skype, captar palavras-passe, introduzir dados no sistema informático visado, bem como ativar o seu *hardware,* possibilitando utilizar o microfone e a *webcam* para gravar sons e tirar fotos que sucessivamente serão enviadas para as entidades responsáveis pela investigação.[262]

[261] *Idem*, p. 328.
[262] RAMALHO, David Silva, 2013, p. 219.

Entretanto, e aqui está a grande questão, é que apesar do entendimento do Tribunal Constitucional Federal e do caráter excecional previsto na Lei quanto às possibilidades de instalação e utilização do *malware*, há notícias que o *Bundestrojaner* foi utilizado mais de cinquenta vezes, sem que a sua instalação tenha se limitado aos casos de terrorismo, o que demonstra o desrespeito não só com os requisitos previstos na Lei, mas também com os cidadãos alemães.[263]

### 3. A atual situação espanhola e o projeto HIPCAR

Até pouco tempo atrás a Espanha não contava com nenhuma legislação especifica sobre a admissibilidade do uso de *malware* como meio de obtenção de prova. Entretanto, mesmo sem previsão legal expressa, a sua inadmissibilidade não era pacifica na doutrina e na jurisprudência.

Parte da doutrina espanhola, como Eloy Velasco Nuñes, entendia ser admissível o uso de *malware* com base na aplicação analógica do regime das interceptações de comunicações eletrônicas ou magnéticas, à luz da jurisprudência do Supremo Tribunal e do Tribunal Constitucional da Espanha.[264]

Em sentido contrário, Ortiz Pradillo apresentava uma critica a tendência da jurisprudência em se substituir pelo legislador, considerando inadmissível uma interpretação que busque legitimar o uso de *malware* nos meios de obtenção de prova previstos na *Ley de Enjuiciamento Criminal* (LEC). Entretanto, o autor referia que se a jurisprudência pretendia admitir o uso de *malware* como meio de obtenção de prova, deveria fazê-lo com a respectiva previsão dos requisitos para tanto. Nesse sentido, o autor entende ser requisito essencial para o uso de *malware* no contexto de investigações criminais: a obrigatoriedade de precedência de mandado judicial fundamentado; exigência da natureza secreta da medida; obrigatoriedade da cooperação de terceiros, como operadoras de telecomunicações, quando necessário; a excecionalidade da medida e respectiva aplicação somente a crimes graves; e a recolha das informações de modo a assegurar sua autenticidade e integridade.[265]

Mas a urgência e importância da matéria fizeram com que a tarefa de estabelecer requisitos para o uso de *malware* não ficasse a cargo da jurisprudência. O

[263] *Ibidem.*
[264] NUÑEZ, Eloy Velasco, *ADSL y Troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal*, La Ley Penal, nº 82, 2011, p. 24.
[265] PRADILLO, Juan Carlos Ortiz. 2011, p. 78.

legislador espanhol aprovou recentemente a reforma da *Ley de Enjuiciamento Criminal*, por via da *Ley Organica* 13/2015, que inclui um capítulo dedicado ao uso de *malware* e tecnologias similares em sistemas informáticos, onde consta uma regulação detalhada dos pressupostos, requisitos e limites de duração para o seu uso, bem como a previsão de um dever de colaboração de terceiros (fornecedores de serviço).[266] Nessa linha, o art. 558° *septies*, *a*, n° 1, prevê, mediante prévia autorização judicial:

> "a utilização de dados de identificação e códigos, assim como a instalação de um *software*, que permitam, de forma remota e telemática, o exame à distância e sem conhecimento do seu titular ou do utilizador do conteúdo de um computador, dispositivo eletrônico, sistema informático, instrumento de armazenamento em massa de dados informáticos ou base de dados, sempre que prossiga a investigação de algum dos seguintes crimes: a) crimes cometidos no seio de organizações criminosas; b) crimes de terrorismo; c) crimes cometidos contra menores ou pessoas com capacidade modificada judicialmente; d) crimes contra a Constituição, de traição e relativos á defesa nacional; e) crimes cometidos através de sistemas informáticos ou de qualquer outra tecnologia de informação ou telecomunicação ou serviço de comunicação".

Ademais, pode-se dizer que as demais alíneas referentes ao uso dessas medidas parecem satisfazer os requisitos propostos por Ortiz Pradillo, o que leva a crer que o ordenamento jurídico espanhol ganhou em termos de clareza e segurança na aplicação deste tipo de medida.[267]

Por fim, devemos mencionar o projeto *Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean* (HIPCAR), lançado em 2008 pela Comissão Europeia e a *International Telecommunication Union* (ITU), com o propósito de estimular a uniformização da legislação nos países da Comunidade das Caraíbas (CARICOM) em áreas relacionadas com a tecnologia de informação. Como resultado, surgiu possivelmente o mais detalhado modelo legislativo em matéria de cibercrime e prova digital existente, que no artigo 27º do *Cybercrime/e-Crimes Model Policy Guidelines in Legislative Texts*, prevê, exatamente, o uso de *malware* em sede de investigação criminal (aí chamado de *remote forensic software*). Como requisitos para sua utilização, a norma prevê a exigência de que a prova não possa ser obtida de outra forma, a necessidade de precedência de autorização por parte de juiz ou magistrado, a exigência de densificação da autorização concedida e a limitação do seu âmbito de aplicação. A norma se mostra um bom exemplo para os Estados que pretendam integrar

[266] RAMALHO, David Silva, 2017, p. 333-334.
[267] *Idem*, p. 334-335.

este meio de obtenção de prova no seu catálogo processual, pecando apenas na necessidade de mero despacho por autoridade judiciaria para autorizar a medida (e não necessariamente judicial) e na ausência de exigência expressa da junção aos autos do relatório de utilização do *malware* (o que fere o contraditório e a ampla defesa).[268]

Do exposto, fica demonstrada a crescente popularidade que o uso de *malware* como meio de obtenção de prova vem ganhando em diversos Estados (tendo em vista suas claras vantagens). Ainda, considerando que o Estado que o visado atua pode não ser o Estado em que o resultado típico se produz, e uma vez que a utilização destes instrumentos de investigação está limitada pelo princípio da territorialidade da aplicação da lei processual penal, aumentam os interesses para que meios mais eficazes de obtenção de prova (como o *malware*) se encontrem consagrados uniformemente no maior número possível de Estados (como no projeto HIPCAR), ajudando no combate a cibercriminalidade, a qual vem se aperfeiçoando cada vez mais.

## 4. Enquadramento conceitual e legal do uso de malware como meio de obtenção de prova no ordenamento jurídico Português segundo a Lei do Cibercrime

Não há referência expressa sobre o uso de *malware* como meio de obtenção de prova no ordenamento jurídico Português. Mas com o intuito de avaliar sua admissibilidade e legitimidade, a doutrina e jurisprudência vêm fazendo certas reconduções aos meios de obtenção de prova elencados na Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro). Em alguns casos, tentam faze-la com fundamento em uma aplicação direta do regime da interceptação de comunicações, previsto no art. 18º da Lei; em outros, numa aplicação deste regime mesclado com o regime das buscas; outros, na aplicação do regime da pesquisa de dados informáticos, previsto no art. 15º da Lei do Cibercrime; e por fim, também há aqueles que buscam legitima-la com base na figura do já estudado agente encoberto em ambiente digital, previsto no art. 19º, n. º 1 da Lei do Cibercrime.

Nessa linha, importante ter presente que as regras de direito probatório previstas na Lei do Cibercrime não são meras normas processuais sobre cibercrimes ou sequer apenas relativas a crimes praticados em sistemas informáticos, mas dizem respeito a um regime consideravelmente mais abrangente sobre prova eletrônica em

[268] *Idem*, p. 336.

processo penal aplicável a *qualquer crime* (com exceção dos artigos 18º e 19º, que são meios de prova específicos para o combate de determinados tipos de crimes).[269]

Porém, antes de analisarmos a possibilidade de as figuras acima legitimarem ou não o uso de *malware*, se faz importante apresentarmos a delimitação conceitual feita pela doutrina sobre o tema. A grande maioria dos autores, assim como o ordenamento jurídico Alemão, ao referir sobre o uso de *malware* como meio de obtenção de prova, o faz sob a terminologia *busca online*. Segundo Manuel da Costa Andrade, as buscas online tratam-se de um "conjunto de intromissões nos sistemas informáticos, feitas através da *internet* e que se actualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas informáticos"[270].

Em sentido semelhante, Paulo Pinto de Albuquerque entende que

> "a busca online consiste na infiltração electrónica em sistemas informáticos, por exemplo, através dos chamados cavalos de Tróia, de modo a que o investigador possa em tempo real ou deferido conhecer a informação que está a ser introduzida ou já foi introduzida no sistema, incluindo textos, sons e imagens"[271].

Todavia, ainda que tais conceitos se encaixem em grande parte com a proposta oferecida pelo uso de *malware* como meio de obtenção de prova, para David Silva Ramalho[272], a terminologia usada, *buscas online*, se mostra errônea. Primeiramente, porque não se esta perante uma situação de busca, e depois, porque, não é necessário que a instalação de *malware* ou a recolha de informação por esse *software* ocorra online (como demonstrado anteriormente).[273]

A busca *domiciliária*, prevista no art. 174º e seguintes do CPP, não pode ser comparada com a busca online, pois ao contrário daquela, onde é entregue ao investigado o mandado de busca e o mesmo pode verificar o seu cumprimento, sendo considerado um meio "aberto" de obtenção de prova, nessa, o suspeito não sabe que está sendo investigado, muito pelo contrário, o secretismo é absoluto e indispensável para a realização da medida, motivo pelo qual é considerado como um método oculto de

[269] MESQUITA, Paulo Dá, Processo penal, prova e sistema judiciário, Coimbra: Coimbra Editora, 2010, p. 98.
[270] ANDRADE, Manuel da Costa. 2009, p. 166.
[271] ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 4º edição, Universidade Católica Portuguesa, Lisboa, 2011, p. 502.
[272] RAMALHO, David Silva. 2013, p. 199.
[273] Ainda que o referido autor discorde da terminologia *buscas online* para se referir ao uso de *malware* como meio de obtenção de prova, seguiremos a maioria da doutrina e também a usaremos.

obtenção de prova.[274] Nesse sentido, o Tribunal de Justiça Federal da Alemanha (BGH) proferiu a seguinte decisão em 31/01/2007 sobre as buscas online:

> "Comparada com as buscas abertas, reguladas nos § 102 ss da StPO, toda a busca oculta configura, por causa da sua elevada intensidade invasiva, uma medida coerciva com um novo e autônomo caráter. A realização a descoberto dá ao atingido a possibilidade de, consoante as circunstâncias, evitar a medida entregando a coisa procurada, limitar sua duração e intensidade; e, para além disso e eventualmente com o apoio de advogado, mesmo durante a execução, opor-se à medida por falta ou ultrapassagem dos pressupostos legais ou, ao menos, controlar a natureza e o modo da busca; e, particularmente, vigiar o cumprimento dos limites impostos pela decisão de autorização. A busca oculta retira ao interessado estas possibilidades".[275]

Em sendo assim, a figura das buscas tradicionais não pode legitimar as buscas online (ou, como preferir, o uso de *malware* como meio de obtenção de prova), pois só pelo fato de serem ocultas, são mais gravosas e invasivas que aquelas, e a sua admissibilidade por essa via seria uma violação ao princípio da legalidade.

Outra questão é no que se refere à interceptação de comunicações, prevista no art. 18º da Lei do Cibercrime, e no regime das escutas telefônicas para o qual remete o seu n. º 4, onde também se busca base legal que permita a instalação de *malware* para obtenção de dados informáticos.

Com a evolução tecnológica, as telecomunicações passaram a abranger os mais variados meios de transmissão (por cabo ou rádio, analógico ou digital) e as mais variadas formas de expressão (palavras, imagens, sons, sinais, etc.), que são enviadas do remente ao destinatário. É nesse contexto que passa incidir o *direito fundamental da inviolabilidade das telecomunicações*. Segundo Manuel da Costa Andrade, o que está em causa aqui é

> "assegurar o livre desenvolvimento da personalidade de cada um através da troca, à distancia, de informações, notícias, pensamentos e opiniões, à margem da devassa da publicidade. O que está em causa é, em última instância, a tutela da privacidade. Mais precisamente, e na formulação do Tribunal Constitucional Federal, da *privacidade à distância.* Porque se trata de comunicação entre pessoas, separadas no espaço, ela tem de ser feita sob mediação necessária de terceiro, isto é, de um fornecedor de serviços de comunicação à distancia, normalmente uma empresa de telecomunicação"[276].

[274] ANDRADE, Manuel da Costa, 2009, p. 115.
[275] *Ibidem.*
[276] *Idem*, p. 158.

Assim, pode-se dizer que a tutela do sigilo de telecomunicações está vinculada ao processamento da comunicação sob o domínio da empresa fornecedora do serviço de telecomunicações. O sigilo só existe enquanto dura o processo dinâmico de transmissão, no momento em que a comunicação é recebida e lida pelo destinatário, termina o processo de telecomunicação à distância. Por exemplo, depois de recebido, lido e guardado no computador do destinatário, um e-mail passa a não pertencer mais à área de tutela das telecomunicações, passando a valer como um normal escrito e sujeito ao mesmo regime que se encontra qualquer ficheiro criado pelo utilizador e arquivado no seu computador. Dessa maneira, se esses arquivos que já se encontram armazenados no computador não podem ser considerados uma telecomunicação e consequentemente não podem ser protegidos pela inviolabilidade das mesmas, não podemos falar no regime da interceptação de telecomunicações para legitimar a sua obtenção via *malware* em uma investigação levada a cabo pelo Estado. Portanto, podemos concluir que a busca online, por não configurar uma invasão ou devassa de um ato de telecomunicação, não está abrangida nem legitimada pelas normas da lei processual relativas ás intromissões nas telecomunicações.[277]

Para corroborar com tal entendimento, David Silva Ramalho muito bem expõem ao fazer referência ao regime da interceptação de comunicações, afirmando que

> "qualquer dos normativos em causa permite que se intercetem comunicações, isto é, que se captem comunicações visadas entre o momento do seu envio pelo remetente e o momento da sua chegada ao destinatário; nunca a monitorização de dados diretamente no aparelho utilizado para as enviar, onde, em rigor [...], não estamos (ou não estamos somente) perante comunicações"[278].

Ainda, devemos levar em conta que as buscas online são um método altamente invasivo utilizado para obter a informação visada diretamente na sua fonte, e que diferentemente da interceptação de comunicações, que tem limitado o tipo de dados a interceptar, nas buscas online dificilmente será possível captar um conjunto especifico de dados. Muito pelo contrário, toda a atividade, lícita ou ilícita, efetuada no computador do investigado ou em torno dele (considerando a hipótese de ativação da *webcam* ou do microfone) poderá ser monitorada, onde, por exemplo, o Estado passará a ter a sua disposição o "diário pessoal" do investigado, com as mais variadas

[277] *Idem*, p. 159-160.
[278] RAMALHO, David Silva, 2013, p. 226.

informações sobre sua vida pessoal e privada, pondo em causa a integridade e confidencialidade do sistema informático.[279]

Todavia, poderia admitir-se o uso de *malware* com base no regime em questão, se o mesmo fosse instalado e utilizado apenas e tão somente para a interceptação de comunicações de áudio realizadas através de "Voice Over Ip", como por exemplo, via Skype, meio de comunicação esse que pelas suas características e baixo custo, está em exponencial crescimento a nível mundial.[280] Mas dificilmente um *malware* conseguiria filtrar suas funções e ser utilizado apenas para isso, e caso o fosse, perderia sua real identidade.[281]

Em uma linha um pouco semelhante, argumenta-se que as escutas ambientais, previstas no art. 189º do CPP, se assemelham e legitimam o uso de *malware*, já que aquelas tratam-se da instalação de meios técnicos em espaços físicos, de modo secreto e com o objetivo de captar conversações diretamente na sua fonte. Porém, uma simples observação é o suficiente para rechaçar tal argumento. A remissão feita pelo legislador no nº 4 do artigo 18º da Lei do Cibercrime para o regime das escutas se restringe tão somente ao "regime de intercepção e gravação de conversações ou comunicações telefônicas constate dos artigos 187º, 188º e 190º do Código de Processo Penal", e não ao regime das escutas ambientais prevista no art. 189º, o qual foi excluído pelo legislador.[282]

Outra corrente, liderada por Paulo Pinto de Albuquerque[283], afirma que a busca online se encontra consagrada no art. 15º da Lei do Cibercrime, que prevê a já tratada pesquisa em sistema informático. A medida é utilizada quando seja necessária a obtenção de dados informáticos específicos e determinados, armazenados num determinado sistema informático, e manda aplicar, com as devidas ressalvas, o regime relativo ás buscas previsto no Código de Processo Penal.

Em sendo assim, o art. 176º nº 1 do CPP passa a ser aplicável ás pesquisas de dados informáticos, tornando exigível que o visado tenha conhecimento da busca e em que termos ela ocorrerá, podendo acompanhar a totalidade da diligência. Na presença de tais requisitos, a pesquisa de dados informáticos, assim como as buscas tradicionais, pode ser designada como um meio aberto de obtenção de prova, não podendo ser

[279] *Ibidem.*
[280] VENÂNCIO, Pedro Dias, Lei do Cibercrime – Anotada e comentada, Coimbra editora, 1º edição, 2011, p. 119.
[281] Sobre isso, ver: ANDRADE, Manuel da Costa, 2009, p. 164-166.
[282] RAMALHO, David Silva, 2013, p. 226-227.
[283] ALBUQUERQUE, Paulo Pinto de, 2011, p. 502.

assemelhado com a busca online, que como vimos, é um meio oculto de investigação. Ainda, essa remissão feita ao regime das buscas, indica claramente que a pesquisa é sempre efetuada fisicamente no próprio sistema, e não pela instalação por via remota de qualquer *software* no computador do investigado. Como se isso não bastasse, o nº 1 do art. 15 da Lei do Cibercrime refere sobre a obtenção de dados informáticos "*específicos e determinados, armazenados num determinado sistema informático*", o que exclui, desde logo, a obtenção genérica de dados em tempo real proporcionada pela busca online.[284]

Importante analisar também o já referido nº 5 do art. 15, que prevê a admissibilidade da extensão da pesquisa informática a sistemas acessíveis através de outro sistema que seja inicialmente objeto da pesquisa. Mas este normativo também não vem permitir a realização de buscas online, mas sim apenas uma extensão do mandado sempre que os dados visados se encontrem em outro sistema informático e desde que seja legitimo o seu acesso através do sistema original (como por exemplo, dados armazenados em nuvem[285]), e não através da instalação de um novo *software* de investigação (*malware*) realizado à revelia do visado. Ainda, o acesso ao primeiro sistema informático compromete o secretismo da diligência, permitindo ao visado o controle da sua legalidade.[286]

Assim sendo, resta concluso pela inaplicabilidade do regime da pesquisa em sistema informático para sustentar a utilização de *malware* no contexto de investigações criminais em ambiente digital.[287]

Finalmente, devemos nos debruçar no art. 19º da Lei do Cibercrime, onde o legislador português (apesar de nada constar na Convenção do Cibercrime ou da Decisão Quadro nº 2005/222/AI) tomou a iniciativa de legislar sobre a possibilidade de recurso a ações encobertas no âmbito da criminalidade informática. O referido art. prevê que é admissível o recurso ás ações encobertas previstos na Lei nº 101/2001, de 25/09 (o já mencionado regime jurídico das ações encobertas) no decurso de inquérito relativo a determinados crimes, e sendo necessário *o recurso a meios e dispositivos*

[284] RAMALHO, David Silva, 2013, p. 228.
[285] Sobre isso, ver: RAMALHO, David Silva, A recolha da prova em sistemas de computação em nuvem. In Revista de direito intelectual, Nº 2, Coimbra, 2014, p. 123-162.
[286] CORREIA, João Conde, 2014, p. 42.
[287] RAMALHO, David Silva. 2017, p. 343. Nesse mesmo sentido, Neves entende que a presença da autoridade judiciária durante a pesquisa de dados informáticos (art. 15º nº 1, da Lei 109/2009), bem como as formas de apreensão de dados informáticos (art. 16º, nº 7, alíneas a) a d)) impedem a realização de buscas online. NEVES, Rita Castanheira, As ingerências nas comunicações electrônicas em processo penal, Coimbra, Coimbra Editora, 2011, p. 284.

*informáticos*, devem ser observadas, naquilo que for aplicável, as regras previstas para a interceptação de comunicações.

A partir disso, David Silva Ramalho[288] entende que estaria suficientemente legitimado o uso de *malware* no curso de investigações criminais. O autor afirma que quando o legislador usa a expressão "meios e dispositivos informáticos", não está se referindo a qualquer um dos meios de obtenção de prova previstos na legislação portuguesa, e com isso está legitimando o recurso a outros meios e dispositivos informáticos não previstos na lei, incluindo aí o *malware*. Para melhor elucidar a questão, trazemos as palavras do autor:

> "Perguntar-se-á, então, novamente, que 'meios e dispositivos informáticos' serão estes? A resposta, como se viu, implica que tenhamos em consideração que se trata de meios e dispositivos que não encontram previsão expressa na lei processual penal portuguesa por cujo caráter excecional, invasivo e insidioso possa ser comparado e condicionado ao recurso ao agente encoberto e cujo funcionamento possa ser regulado e limitado pelo regime da interceção de comunicações. Trata-se, a nossa ver, da consagração da utilização (que incluirá, naturalmente, a instalação) de *malware* como método oculto de investigação criminal em ambiente digital"[289].

No que se refere ao caráter particularmente gravoso dessa medida, o autor entende que a remissão ao regime excepcional das ações encobertas justifica-o e legitima-o, pois dessa maneira apenas poderá ser aplicado "se necessário", bem como "se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter". Ainda, a medida deve ser precedida de despacho fundamentado do juiz de instrução a proferir mediante requerimento do Ministério Público (art. 18º, n.º 2, aplicável *ex vi* artigo 19.º, n.º 2, da Lei do Cibercrime). Outros requisitos são elencados para utilização da medida: adequação aos fins de prevenção e repressão criminais identificados em concreto e proporcionais, quer a essas finalidades, quer à gravidade do crime sob investigação (art. 3º, nº 1, da Lei nº 101/2001); fundadas suspeitas da prática de um dos crimes previstos na Lei do Cibercrime ou de crimes cometidos por meio de um sistema informático cuja pena em abstrato seja superior a cinco anos, ou, se inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas

[288] RAMALHO, David Silva, 2013, p. 229-233, bem como em RAMALHO, David Silva, 2017, p. 343-346.
[289] RAMALHO, David Silva, 2017, p. 345-346.

comunicações, a discriminação racial, religiosa ou sexual, as infrações econômico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos (art. 19º, nº 1, da Lei do Cibercrime); e como último requisito, a delimitação dos dados que se visa obter, de acordo com as necessidades concretas da investigação (art. 18º, n.º 3 da Lei do Cibercrime).[290]

Respeitados esses requisitos, o autor entende que nada obstaria, no plano do direito constituído, a utilização de *malware* como meio de obtenção de prova. Entretanto, ainda que essa nos pareça ser a opção mais próxima de legitimar as buscas online no ordenamento jurídico português, não nos parece ser suficiente e adequada.

Primeiramente, porque quando o legislador refere sobre a necessidade de *recurso a meios e dispositivos informáticos* (art. 19º n.º 2 da Lei do Cibercrime), o faz sob remissão ás regras referentes ao regime de interceptação de comunicações (art. 18º da Lei do Cibercrime). Assim, não se pode falar que a expressão "meios e dispositivos informáticos" está se referindo a meios de obtenção de prova não previstos na lei portuguesa, já que faz referência expressa ao regime de interceptação de comunicações. E como exposto anteriormente, tal regime não oferece, de maneira alguma, supedâneo legal ao uso de *malware*.[291]

Analisemos o art. 18º n.º 3, da Lei do Cibercrime, que expõem que a "intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego[292]". Momento algum é feito referência à arquivos já armazenados no computador ou sobre a vigilância e monitorização de dados em tempo real, que é a verdadeira função do *malware*, tendo em vista que o mesmo permite aos investigadores saberem até mesmo quais teclas o visado esta digitando no momento em que são pressionadas (por meio de *keyloggers*), de modo que o que escreve apenas para si e não em um contexto de comunicações (como um lembrete ou um diário pessoal) passará a ser do conhecimento dos investigadores.

Para corroborar com o exposto, trazemos as palavras de Eduardo Bolsoni Riboli, que refere que:

---

[290] *Idem*, p. 355. Bem como em RAMALHO, David Silva. 2013, p. 232.
[291] Nesse sentido: RIBOLI, Eduardo Bolsoni. 2018, p. 73.
[292] Segundo o art. 2º, c), da Lei de Cibercrime, dados de tráfego são os "dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, a duração ou o tipo de serviço subjacente".

> A simples previsão legal com remissão ao regime da interceptação de comunicações quando houver necessidade de suplementação é exígua. Além de serem meios de obtenção de prova nitidamente distintos, aquele regime não contém disposições específicas ao funcionamento de um *software* de espionagem (como as funções que podem ser ativadas, o modo como deve ser realizada a obtenção das informações ou então a instalação e remoção do sistema informático ou dispositivo eletrônico investigado). O alarmante potencial lesivo a direitos fundamentais decorrentes do uso de *softwares* de espionagem demanda clareza, densidade e precisão na regulamentação deste recurso, o que não ocorre na atual versão da Lei do Cibercrime.[293]

Dessa maneira, acreditamos que a menção ao uso de "meios e dispositivos informáticos" visa essencialmente legitimar o uso desses no âmbito de uma ação encoberta que envolva uma *comunicação* em ambiente digital, já que ela não é uma ação livre quanto aos meios, devendo estes se encontrarem reconhecidos expressamente.

Por exemplo, a ação encoberta em ambiente digital poderá consistir na criação de um perfil falso pelo qual é facilitada a intervenção em um *chat* com vista a obtenção de informações relevantes para a investigação (que seria essencialmente a figura do agente encoberto em ambiente digital estudada no capitulo anterior). Ou seja, pode-se admitir, por via do artigo em questão, que o agente encoberto digital utilize-se do *meio* de criar um perfil falso pelo qual o agente investigador se passará por outra pessoa, "ocultando sua identidade de forma a obter provas para incriminar o suspeito, visando a prevenção ou repressão criminal, através da obtenção de informações pessoais relativas à atividade criminosa por ele praticada"[294].

Ou, ainda que se queira crer que quando o nº 2, do art. 19º, faz referência sobre o recurso a *dispositivos informáticos* esteja referindo sobre o uso de *malware*, devemos ter em mente que tais dispositivos devem visar apenas a *interceptação de comunicações* do visado com outras pessoas, mas nunca poderá ser admitido como um *software* que visa invadir o computador do visado e recolher as mais variadas informações sobre o mesmo e sobre o que ocorre em torno dele, inclusive quando acredita estar sozinho, na privacidade de sua casa.

Por outro lado, por ser o recurso ao *malware* um método que se revela altamente mais danoso e restritivo de direitos fundamentais do que o agente encoberto, não se pode admitir que seja utilizado para prevenção e investigação de crimes com pouca ou nenhuma gravidade, como ocorreria se tal medida fosse legitimada pelas ações encobertas em ambiente digital, ferindo os princípios da proporcionalidade e da

[293] RIBOLI, Eduardo Bolsoni. 2018, p. 73.
[294] GONÇALVES, Fernando, *et al*. O novo regime jurídico do agente infiltrado (Comentado e Anotado – Legislação complementar), Coimbra: Almedina, 2001, p. 91-93.

necessidade.[295] Conforme o acertado entendimento do Tribunal Constitucional Federal Alemão já mencionado, a busca online apenas poderá ser executada quando estiver em causa um interesse jurídico predominantemente importante, como a saúde, a vida, a liberdade, ou a própria raiz ou existência do Estado.

Ainda, pelo simples fato de ser um método oculto de obtenção de prova, o legislador deve prevê-la de forma transparente e suficientemente densificada, não podendo ser admitida sua legitimação por uma remissão genérica "naquilo que for aplicável" para um regime legal que, por sua vez, remete "em tudo o que não for contrariado" para outro regime. Por fim, nos dispositivos que fazem previsão ao agente encoberto em ambiente digital, não há referência expressa sobre a obrigatoriedade de após a medida, o visado ter acesso e conhecimento da mesma, para que assim analise e conteste a legalidade das provas colhidas contra si, o que fere de maneira incontestável o princípio do contraditório e da ampla defesa.[296]

Nesse sentido, importante relembrar do julgamento do caso *Big Brother Watch and Others v. The United Kingdom* pelo Tribunal Europeu dos Direitos do Homem, citado por Riboli. Ainda que aos Estados seja ofertado uma margem de apreciação na escolha dos meios apropriados para suas investigações, a utilização de novas tecnologias em investigações criminais somente deve ser admitida se existe uma regulamentação prévia provida de *qualidade,* visando impedir restrições abusivas e desproporcionais a direitos fundamentais. Contudo, não é o que ocorre na Lei do Cibercrime, que ao contrário dos exemplos legislativos estrangeiros, não prescreve as particularidades referentes ao "meios e dispositivos informáticos" dos quais trata.[297]

Portanto, que uma vez concluído pela inaplicabilidade de qualquer uma das referidas normas para oferecer supedâneo legal que legitime o meio de obtenção de prova em análise, não pode o interprete ignorar os limites legais e constitucionais e criar uma nova norma para ajustar um meio de prova atípico, ainda mais se for um meio oculto de obtenção de prova. A única liberdade referente à escolha dos meios de prova, segundo Paulo de Sousa Mendes, reside na possibilidade de selecionar do catálogo dos meios de prova típicos aqueles que forem considerados como adequados ao processo em curso.[298]

[295] MESQUITA, Paulo Dá, 2010, p. 126.
[296] RAMALHO, David Silva, 2013, p. 234.
[297] RIBOLI, Eduardo Bolsoni. 2018, p. 74.
[298] MENDES, Paulo de Sousa, Lições de Direito Processual Penal, Coimbra: Almedina, 2013, p. 174.

Portanto, a invasão de sistemas informáticos para recolha de dados informáticos e para vigilância da atividade virtual do visado por meio da utilização de *malware*, só poderá ocorrer se legitimada por pertinente e inequívoca previsão legal, e concluído pela sua inexistência, resta forçoso afirmar que tal prática invasiva está revestida por uma invencível proibição de prova no ordenamento jurídico Português.[299]

## 5. A consequente necessidade de previsão e precisão legal do *malware* como método oculto de investigação criminal

O uso de *malware* é possivelmente o meio mais gravoso de obtenção de prova que pode ser consagrado legalmente em um Estado Democrático de Direito. Para Ramalho, representa um elevado nível de danosidade social, onde a monitorização remota de um indivíduo no seu computador traduz-se em uma potencial intromissão no núcleo intangível da intimidade pessoal, ofendendo gravemente os mais variados direitos fundamentais já estudados aqui, como a reserva da intimidade da vida privada, a inviolabilidade do domicilio, o direito a não autoincriminação, a confidencialidade e integridade dos sistemas informáticos, entre outros.[300]

Para situações como essa, conforme o autor, a própria Constituição da República Portuguesa prevê, em seu art. 32º, a nulidade da prova obtida mediante tortura, coação, ofensa a integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicilio, na correspondência ou nas telecomunicações. Corroborando com essa proteção, o art. 126º do CPP, relativo à epígrafe "Métodos proibidos de prova", refere que "ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respectivo titular", o que se traduz em uma garantia processual.

Nesse sentido, não se pode admitir que um meio de obtenção de prova que fere de maneira inquestionável, e talvez até incomparável, a área nuclear e inviolável da intimidade e a confidencialidade e integridade dos sistemas informáticos, explore os silêncios e lacunas da lei e venha a ser legitimado pelo interprete do direito com base nos dispositivos analisados anteriormente, que não dão azo suficiente para que a medida marque presença no quotidiano dos tribunais e dos cidadãos. Mas da mesma maneira,

[299] ANDRADE, Manuel da Costa, 2009, p. 157 e 168.
[300] RAMALHO, David Silva, 2013, p. 233.

não pode o legislador fechar os olhos para esse problema e abrir mão da utilização de um recurso tão eficiente para obtenção de prova, que pode se mostrar como uma verdadeira arma no combate aos tipos mais extremos de criminalidade.

Assim, assumindo as evidentes vantagens do uso de *malware* para descoberta da verdade e da recolha de provas em ambiente digital (levando-se em conta que o uso do mesmo permite contornar as diferentes medidas antiforenses estudadas aqui, já que vigia a atividade em tempo real no sistema informático visado e envia as informações para os investigadores), se mostrando uma ferramenta muito eficiente para a prevenção e repressão das formas mais graves e ameaçadoras da criminalidade (criminalidade organizada e transnacional, terrorismo, etc.), e assumindo sua imprescindibilidade em certos casos, para que seja admitida a limitação e danosidade dos diversos direitos fundamentais que a medida atinge e o Estado ponha o pé virtual na casa do investigado de maneira legitima, encontrando-se assim o equilíbrio da balança, a consagração legal e constitucional da medida deve ser prevista pelo legislador com uma norma lisa, transparente e de especial densidade, com os respectivos pressupostos, requisitos e finalidades da instalação e utilização do *malware* como meio de obtenção de prova no processo penal, respeitando assim o princípio da proporcionalidade, da legalidade e da clareza.

Ademais, pela evidente eficácia desse meio de obtenção de prova digital, que por se inserir em sistemas informáticos pertencentes à um ciberespaço global que sofre diretamente com a limitação imposta pelo princípio da territorialidade da aplicação da lei processual penal, entendemos que a medida em questão merece cada vez mais ser prevista em iniciativas de caráter supranacional, com o intuito de uniformizar os requisitos e a legitimidade da mesma no maior número possível de Estados.

Mas justamente por ser um meio oculto e representar um elevado sacrifício de direitos fundamentais, Costa Andrade entende que não apenas as buscas online, mas todos os meios ocultos de investigação criminal (escutas telefônicas, agentes encobertos, etc.) estão sujeitos a uma intransponível exigência de reserva de lei, sendo admissíveis e válidos apenas se gozam de expressa e específica consagração legal. Com isso, o autor entende que segue a exigência da clareza e determinabilidade, onde a lei deve permitir identificar com segurança e rigor tanto o bem jurídico e o direito fundamental lesado ou atingido como o teor do respectivo sacrifício, além do fundamento, fim e limites da intromissão, estando ela finalisticamente vinculada. Caso não seja assim, nos casos em que se utilize o *malware* para obtenção de prova, o visado

poderá sofrer pesquisas exploratórias e uma monitorização desproporcional, indo além das finalidades da investigação. Assim, por vivermos em uma era de incessante progressão tecnológica, a oferecer constantemente novos meios (ocultos) de investigação, esses terão sua produção e valoração ilegais e ilegítimas enquanto não houver nova e pertinente intervenção do legislador ordinário, não se admitindo o recurso à analogia.[301]

É nessa linha que o autor afirma ser necessária a criação de uma teoria geral das formas ocultas de investigação, tratando-se, fundamentalmente, "de identificar as categorias e definir os princípios normativos basilares, comuns ás diferentes formas típicas de investigação e a sua ulterior aplicação, aberta ás singularidades de cada uma delas".[302] Em outros termos, trata-se de estabelecer os pressupostos gerais que a concreta aplicação das medidas deve obedecer, onde cada meio estará sujeito a exigências acrescidas ou atenuadas, segundo o princípio da proporcionalidade, que sempre deverá basear-se no potencial de lesividade e devassa da medida. Será exatamente sobre essas questões que trataremos no próximo capítulo.

[301] ANDRADE, Manuel da Costa, 2009, p. 112-113. No mesmo sentido, ANDRADE, Manuel da Costa, 2011, p. 540-541.
[302] ANDRADE, Manuel da Costa, 2011, p. 539.

# VI. REGRAS E PRINCÍPIOS GERAIS DOS MÉTODOS OCULTOS DE INVESTIGAÇÃO CRIMINAL

Como já estudado no presente trabalho, cabe ao Estado definir até onde é lícito afetar direitos, liberdades e garantias de cidadãos presumivelmente inocentes para recolha de prova incriminatória em vista de exercer o seu poder punitivo. É em razão disso que a exigência constitucional do princípio do processo justo e equitativo deve visar para a eficiência tanto na defesa dos cidadãos contra abusos do Estado, bem como para a eficiência da legitimação estatal na utilização dos meios à disposição em uma investigação criminal.[303] Assim, em certos casos a eficiência na defesa dos visados pela ação penal produzirá insuperáveis limites para a investigação criminal, enquanto em outros casos a eficiência no plano da investigação criminal legitimará a restrição de direitos fundamentais do visado e a criação de certas exceções processuais.[304]

Os métodos ocultos de investigação surgem justamente no equilíbrio dessas coordenadas/limites, onde o aplicador do Direito deverá se mover no estrito cumprimento das exigências legais e constitucionais aplicáveis, buscando as soluções aceitáveis à luz das circunstâncias de fato e de direito em causa, e excluindo as demais soluções que se mostram desproporcionais. Mas ocorre que esses *limites* não fornecem os necessários critérios de legitimidade para o recurso a certos métodos ocultos de investigação criminal. Ainda, o problema se agrava quando na busca de tais critérios no ordenamento jurídico Português sobre os métodos ocultos, constata-se que não há sequer um esboço de regime geral dos mesmos, existindo, como já visto, sucessivos diplomas sem qualquer unidade sistemática ou de aparente ordem valorativa, criando um verdadeiro caos normativo.[305]

Assim, como afirma David Silva Ramalho, a falta de critérios legislativos de um regime geral e unificado e a existência de comprometedoras inconsistências e assimetrias no direito positivo que regula esta matéria impõem a necessidade de criação de um regime jurídico e uma *teoria geral* dos métodos ocultos. Essa exigência se faz desde logo porque o recurso aos métodos ocultos, enquanto ingerência ou intervenção restritiva de direitos fundamentais, sempre se encontrará sujeita ao regime legal, formal

[303] RAMALHO, David Silva. 2017, p. 211.
[304] COSTA, Eduardo Maia. 2014, p. 358.
[305] RAMALHO, David Silva. 2017, p. 211.

e procedimentalmente delineado, e, nas áreas de maior indeterminação, aos critérios fornecidos pela Lei Fundamental para a aplicação proporcional da norma ao caso.[306]

Assim, a criação de uma teoria geral dos métodos ocultos de investigação visa "identificar as categorias e definir os princípios de investigação e a sua ulterior aplicação, aberta às singularidades de cada uma delas"[307]. Portanto, nas próximas páginas iremos identificar as coordenadas essências e os princípios fundamentais para a legitimação, utilização e escolha dos métodos ocultos no contexto de uma investigação criminal em um Estado de Direito.

## 1. A reserva de lei

Como primeiro pressuposto, devemos trazer a *reserva de lei*, a qual já foi mencionada de maneira breve ao longo do presente estudo, e que resgatamos, a partir do entendimento tecido por Andrade. De acordo com o autor, como significado óbvio, só a lei pode autorizar e legitimar as medidas em questão. Mas tal significado se desdobra em um largo de exigências normativas e de incontornáveis implicações prático-jurídicas. Uma dessas exigências (destacando-se a lição do Tribunal Constitucional Federal Alemão) é a clareza e determinabilidade da lei. Isso significa que a lei deve permitir identificar com rigor e segurança tanto o bem jurídico ou o direito fundamental lesado ou atingido como o teor do respectivo sacrifício. Dessa exigência vai naturalmente coenvolvida a previsão da forma ou modalidade técnica da invasão, o que vem a revelar a importância e relevo de tal exigência, tendo em vista o progresso tecnológico que vem oferecendo permanentemente novos meios (ocultos) de investigação. Assim, a produção e valoração serão ilegais e ilegítimas enquanto não for adotada nova e pertinente lei de autorização.[308]

As leis existentes não podem ser vistas como uma espécie de "normas penais em branco", passíveis de plasticidade e abertas á subsunção de novos meios técnicos de invasão e devassa. Ou seja, as existentes autorizações legais não podem sofrer alargamentos para compressão ou invasão de direitos fundamentais, devendo ser interpretadas e aplicadas no estrito respeito dos seus limites legais. Portanto, o recurso a um novo meio técnico (oculto e invasivo) de investigação em processo penal (buscas

[306] *Idem*, p. 212.
[307] MATA-MOUROS, Maria de Fátima. 2011, p. 37.
[308] ANDRADE, Manuel da Costa. 2009, p. 112.

online, por exemplo) somente é possível depois de prévia, explícita e autônoma legitimação legal. Nesse sentido, além de identificar o direito atingido e demarcar rigorosamente a medida da agressão permitida, a lei deve prever e prescrever também de forma precisa e com clareza normativa o fundamento, o fim e os limites da intromissão. Ou seja, a intromissão legalmente autorizada está finalistiscamente vinculada, o que obriga o legislador a determinar de forma precisa o fim da recolha de dada informação.[309]

Para ilustrar, trazemos o exemplo citado por Pradillo do caso *Vetter vs. França*, de 31 de maio de 2005, onde a autorização judicial para a entrada e instalação de microfones pela polícia em um domicílio foi declarada vulneradora da legalidade devido a ausência de regulação legal sobre a matéria, já que a legislação francesa não previa expressamente tal medida investigativa. Contra a postura do governo francês, segundo o qual a legislação francesa permitia a intervenção de comunicações emitidas ou recebidas por meios telemáticos, o TEDH (Tribunal Europeu dos Direitos Humanos) sentenciou que tais disposições não serviam de base legal para proceder a instalação de microfones em lugares privados por falta de "qualidade da lei", isto é, porque a lei deve utilizar termos o suficientemente claros para que qualquer um compreenda em que circunstâncias e condições habilita aos poderes públicos realizar determinado atentado secreto e virtualmente perigoso para o direito ao respeito da vida privada e da correspondência.[310]

Á reserva de lei são acrescidos outros pressupostos ou exigências complementares e cumulativos. Um deles é o *catálogo* de infrações cuja perseguição pode legitimar cada um dos meios ocultos em causa. Levando em conta a elevada danosidade social que os meios ocultos implicam, esse catálogo deve ser sempre particularmente restrito e definido segundo critérios de *proporcionalidade*: tanto na direção da gravidade das infrações como das exigências criminalísticas da sua investigação. Em razão disso, não seria proporcional um quadro normativo que autorizasse a utilização de um meio particularmente invasivo para investigar um crime de pouca ou nenhuma gravidade, para o qual sequer estivessem previstos meios menos gravosos. A mesma crítica deve ser feita da solução legal que alargasse os meios mais gravosos e invasivos de investigação a um universo mais alargado de infrações, de

[309] *Idem*, p. 113.
[310] PRADILLO, Juan Carlos Ortiz. "*El impacto de la tecnología en la investigación penal y en los derechos fundamentales"*. 2013, p. 335.

menor gravidade e relevo, como ocorreria se fosse admitido o uso de *malware* por via do art. 19º da Lei do Cibercrime, por exemplo.[311]

Assim, o catálogo de crimes que eventualmente legitime a utilização do *malware* terá de ser mais reduzido, por exemplo, do que o catálogo do agente encoberto em ambiente digital, limitando-se aquele aos casos mais graves, onde os outros meios de obtenção de prova se revelem ineficazes. E aqui reforçamos o nosso entendimento, em consonância com o Tribunal Constitucional Federal Alemão, que as buscas online devem caber para investigação e luta de um catálogo muito limitado de crimes, como terrorismo, crime organizado e crimes contra a vida.[312]

Por segundo, ainda que verificada a investigação e perseguição de algum dos crimes do *catálogo,* a admissibilidade do meio oculto irá depender também da verificação em concreto de uma *suspeita fundada* da ocorrência da infração. Tal suspeita deverá ser baseada em fatos concretos e definida segundo limiares de plausibilidade ou probabilidade, graduados (suspeita simples, suspeita forte, etc.) em função do potencial de devassa do meio. Ou seja, se o meio oculto tem um elevado potencial de devassa, a suspeita do crime que se investiga com recurso ao mesmo deve ser elevada também (por ser o recurso a *malware* de grande devassa, grande deverá ser a suspeita).[313]

Ainda, o juízo de suspeita deve reportar-se ao momento em que a autoridade competente decide sobre a autorização ou recusa da medida. E segundo Costa Andrade, é também esse o

> "momento que há-de reportar-se a instância de recurso a seu tempo chamada a escrutinar a legalidade e validade da medida. Instância que, por vias disso, não pode entrar em linha de conta com o reforço da plausibilidade da suspeita, entretanto trazido pela efectiva realização da medida e pelo aproveitamento do seu potencial heurístico."[314]

Ou seja, caso venha a recorrer sobre o preenchimento dos requisitos que deram causa a medida investigativa, o acusado irá basear-se no momento em que a medida foi autorizada e no grau de suspeita que existia até então, tendo em vista que caso fosse basear-se em momento posterior, o grau de suspeita poderia já ter sido transformado em um grau de certeza do cometimento do ilícito em investigação.

---

[311] ANDRADE, Manuel da Costa, 2009, p. 114.
[312] No mesmo sentido: CORREIA, João Conde. 2014, p. 44.

[313] ANDRADE, Manuel da Costa, 2009, p. 114.
[314] *Ibidem.*

## 2. Princípio da subsidiariedade

Os métodos ocultos deverão respeitar também um princípio de *subsidiariedade*, o qual deve ser observado tanto no plano extrínseco, ou seja, na relação com os meios "abertos" de investigação, como no plano intrínseco (com os próprios meios ocultos entre si). Dessa maneira, não deve nunca recorrer-se a meios ocultos quando for possível alcançar os mesmos resultados de investigação com a aplicação de meios abertos/descobertos. Os meios ocultos de investigação são, por si só e pelo simples fato de serem ocultos, mais gravosos do que os meios abertos. Assim, tendo em vista que a intensidade de devassa de um meio de intromissão é determinada pelo seu secretismo, em um Estado de Direito a ocultação das medidas estaduais de investigação deve ser a exceção e carece de especial justificação e subsidiariedade, devendo recorrer sempre que possível, primeiramente aos meios abertos de investigação, para então, se necessário for, socorrer-se dos métodos ocultos.[315]

Já no que diz respeito às relações dos meios ocultos entre si, a *subsidiariedade* veda a utilização de um meio oculto de investigação sempre que for possível a utilização de um outro meio oculto menos gravoso e igualmente idôneo para a prossecução dos interesses da investigação. Por exemplo, não se deve recorrer à gravação de conversa entre presentes se no caso puder recorrer-se à gravação telefônica. Sobre isso, Costa Andrade sustenta que "nuns casos bastará que, sem a medida, a investigação fique mais *difícil*; noutros exigir-se-á que ela seja *consideravelmente mais difícil*; noutros, mesmo impossível"[316] (e acreditamos que nesse último se insere o uso de *malware*).

Além disso, o princípio da *subsidiariedade* deve vedar e contrariar a utilização *cumulativa* de dois ou mais meios ocultos de investigação. A utilização de duas ou mais medidas (escutas e agente encoberto, por exemplo) somente poderá ocorrer se a utilização de uma só não permitir alcançar o desejável e almejado resultado probatório. E de qualquer forma, a cumulação de meios ocultos de investigação só deverá acontecer face às manifestações extremadas da criminalidade (tendo em vista a danosidade e

[315] *Idem*, p. 114-115.
[316] ANDRADE, Manuel da Costa. 2011, p. 546.

sofisticação dos meios ocultos), e sempre em consonância com as exigências da proporcionalidade.[317]

### 3. Princípio da proporcionalidade

Os meios ocultos de investigação devem obedecer também o princípio da *proporcionalidade* (o qual, como referido, deve ser respeitado nas demais questões vistas até aqui, como catálogo, limiar de suspeita ou subsidiariedade) visando evitar o abuso, o arbítrio ou o excesso dos fins de uma investigação criminal, onde frequentemente, em razão da busca da verdade e da justiça, há restrição de direitos fundamentais do suspeito ou arguido. Ou seja, a legitimidade do sacrifício de direitos fundamentais em função da prossecução de outro interesse ou fim com dignidade constitucional deverá ser encontrada com recurso a critérios de proporcionalidade, primeiro pelo legislador na configuração dos seus pressupostos, e depois pelo aplicador na sua atividade prática.[318]

Nas palavras de Reis Novais, o princípio da proporcionalidade surge como

> "a referência fundamental do controlo da actuação dos poderes públicos em Estado de Direito, assumindo, particularmente no âmbito dos limites aos direitos fundamentais, o papel de principal instrumento de controlo da actuação restritiva da liberdade individual e de *chave* sem a qual, integrada no recurso á metodologia da ponderação de bens, não seria possível decifrar os complexos problemas que aí vêm suscitados".[319]

Nessa linha, o princípio da proporcionalidade pode ser divido em três vertentes ou subprincípios: (a) o princípio da adequação ou da idoneidade; (b) o princípio da necessidade ou da exigibilidade e (c) o princípio da proporcionalidade em sentido estrito. O princípio da adequação ou da idoneidade significa que as medidas restritivas legalmente previstas devem ser adequadas a realizar os fins visados pela lei. Ou seja, nessa primeira análise de controle é apenas necessário verificar se a medida restritiva (como por exemplo, o uso de *malware*), é objetivamente adequada para a prossecução do fim visado (que neste caso, é a descoberta da verdade material e a realização da justiça). Assim, julgando pela amplitude de possibilidades que o *malware* ou o agente

[317] ANDRADE, Manuel da Costa, 2009, p. 115.
[318] RAMALHO, David Silva. 2017, p. 226-227.
[319] NOVAIS, Jorge Reis. Os princípios constitucionais estruturantes da República Portuguesa, Coimbra: Coimbra Editora, 2004, p. 161.

encoberto em ambiente digital colocam ao serviço da investigação criminal, dificilmente se poderia concluir pela inadequação ou inidoneidade destes meios.[320]

Em um segundo momento importa verificar se a medida restritiva em análise se afigura como *necessária*, no sentido em que os fins visados pela lei não poderiam ser obtidos por outros meios menos onerosos para os direitos, liberdades e garantias. Para isso, deve-se averiguar se não existe outro meio, que sendo igualmente idóneo para prossecução dos fins visados, seja sensivelmente menos gravoso. Tal princípio da necessidade se confunde com o já mencionado princípio da subsidiariedade. Assim, como deverá acontecer relativamente a qualquer método oculto de investigação criminal, a *necessidade* do meio terá que se aferir relativamente a um determinado grau de suspeita do cometimento do crime e a um concreto catálogo de infracções criminais que pretendem legitimar a medida, nomeadamente um catálogo de crimes que se apresentem como suficientemente gravosos, pois como referido, a verdade material não pode ser obtida a qualquer custo.[321]

Importante mencionar que da análise do princípio da necessidade diante do uso de *malware*, parece que o mesmo cumpre perfeitamente tal exigência em determinados casos, tendo em vista que pela dificuldade e peculiaridade na obtenção da prova digital, aliada ao uso de medidas antiforenses, o uso de *malware* se mostra como o único meio capaz de contornar certas situações concretas e obter a prova visada, tendo em vista que a Lei do Cibercrime não revela meios de obtenção de prova suficientes para certos casos, não restando alternativa se não a *necessidade* do uso de *malware*.

Porém, para legitimar qualquer método oculto, é necessário também o respeito ao *princípio da proporcionalidade em sentido restrito*, que significa que os meios legais restritivos e os fins obtidos devem situar-se em uma "justa medida", visando impedir a adoção de medidas desproporcionais em relação aos fins obtidos. Ou seja, trata-se, segundo Novais, "comparar sacrifícios (da liberdade individual) e benefícios obtidos ou visados, vantagens e desvantagens da restrição objecto do controlo."[322]

Assim, é necessário verificar, por exemplo, se o sacrifício imposto ao direito à reserva da intimidade da vida privada não é desproporcional em relação ao benefício que se espera obter com a utilização de *malware* em uma investigação criminal. Nessa

[320] ANDRADE, Manuel da Costa, 2009, p. 116.
[321] DA SILVEIRA, Maria Ana Barroso de Moura. *Da problemática da investigação criminal em ambiente digital - em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova*, Dissertação de Mestrado orientada pelo Professor Doutor Germano Marques da Silva, Universidade Católica Portuguesa: Lisboa, 2016, p. 40.
[322] NOVAIS, Jorge Reis. 2004, p. 179.

linha, como já demonstrado anteriormente as diversas funções do *malware* e os direitos fundamentais que atinge, evidenciando a elevada danosidade social do mesmo, reforça-se a conclusão de que o mesmo apenas seria cabível para investigação/prevenção da mais grave criminalidade e quando estritamente necessária.

Portanto, nestes casos excepcionais, a restrição do direito fundamental à reserva da intimidade da vida privada respeita o princípio da proporcionalidade, não se afigurando excessiva, porquanto aqui a descoberta da verdade material apresenta como fim último acautelar valores constitucionais superiores, nomeadamente a vida e integridade física dos cidadãos, a realização do Estado de Direito e a realização da Justiça. Já nos parece excessiva a sua utilização para a investigação de crimes de menor gravidade, pois a relação entre o prejuízo para os direitos fundamentais dos suspeitos ou arguidos e o benefício que resultaria da restrição se apresenta como inadequada e, como tal, desproporcionada.[323]

## 4. Reserva de juiz

Outra exigência que se faz sentir é referente á entidade competente para decidir sobre a medida ou autorizar a sua realização. Essa competência deve sempre ser reservada ao Juiz, ressalvadas as situações de "perigo de demora". A *reserva de juiz* trata-se fundamentalmente de assegurar a tutela preventiva dos direitos de uma pessoa (normalmente o arguido) exposta à invasão e à devassa sem qualquer possibilidade de assegurar sua própria defesa. Além disso, os métodos ocultos tratam-se de medidas cuja danosidade é certa (e drástica) e cujas vantagens são incertas e aleatórias. Assim, isso tudo vem a justificar a intervenção de uma autoridade independente e neutra.[324]

Portanto, ao juiz, enquanto entidade imparcial, desinteressada e descomprometida no processo, cabe analisar objetivamente os bens jurídicos em conflito nos termos da lei e da Constituição e, perante a proposta do MP para utilização de algum método oculto de obtenção de prova, decidir pela justificação casuística da restrição de direitos fundamentais. A imposição de fundamentação por parte do juiz serve também para tornar a autorização da medida objeto idôneo de futuro escrutínio em sede de julgamento ou de recurso, caso venha a ser questionada a legalidade da mesma e a existência ou não de uma proibição de valoração das provas através dela alcançadas.

[323] DA SILVEIRA, Maria Ana Barroso de Moura. 2016, p. 44.
[324] ANDRADE, Manuel da Costa. 2009, p. 117.

Nesse sentido, por poder ser contestada apenas após a sua própria execução, e depois de ter supostamente aumentado os conhecimentos sobre a suspeita que a deu início, eventual recurso sobre a admissibilidade e legalidade da medida versará a esse momento de autorização da mesma, com base no estado em que se encontrava a investigação, ficando fora de consideração os conhecimentos ulteriormente adquiridos, principalmente os obtidos por meio dela.[325]

Ou seja, incumbe ao juiz uma função de *representação compensatória* do arguido, analisando criticamente os argumentos apresentados para a concessão da autorização judicial e contrabalançando-os com os interesses e direitos do visado, ou seja, deve o juiz ponderar os argumentos que a pessoa atingida poderia invocar se tal possibilidade lhe fosse dada.[326]

Portanto, além de preocupar-se com cumprimento de todos os pressupostos que a lei constitucional e ordinária fazem depender da imposição da medida, como órgão de controle das autoridades de investigação, o juiz deve assegurar, na medida do possível, que a intromissão nos direitos fundamentais se mantenha sempre mensurável e controlável. Assim sendo, na falta ou insuficiência de fundamentação, a resposta deverá ser a ilegalidade da medida e a proibição de valoração dos meios de prova tornados possíveis pela mesma.[327]

Tal postura do juiz se faz importante também pelo fato de que ao mesmo chega apenas a versão mediatizada pelos interessados na investigação, correndo o risco de o juiz figurar aqui reduzido ao estatuto de *longa manus* do Ministério Público, assumindo a sua versão dos fatos e chancelando as suas pretensões. Contudo, infelizmente é isso que de fato tem se observado na prática, onde dados empíricos demonstraram a propensão para, em praticamente todos os casos, o juiz decidir conforme o solicitado pela acusação e autorizar a medida visada. Em razão disso, aumentam as vozes de frustração e desencanto em face da falência generalizada das expectativas colocadas na reserva de juiz.[328]

[325] *Idem,* p. 118.
[326] *Ibidem.*
[327] ANDRADE, Manuel da Costa, 2011, p. 548-549.
[328] ANDRADE, Manuel da Costa. 2009, p. 119.

## 5. Inviolabilidade da *área nuclear da intimidade,* os conhecimentos fortuitos advindos de investigações criminais em ambiente digital e outros requisitos dos métodos ocultos

Como já estudado ao longo do presente trabalho, principalmente a partir da lição da jurisprudência alemã, o direito dos meios ocultos de investigação criminal tem de integrar soluções normativas indispensáveis para garantir a salvaguarda e a inviolabilidade da *área nuclear da intimidade,* bem como definir medidas para tutelar o *direito a recusar depoimento* que no direito processual "aberto" é reconhecido ás testemunhas, seja em nome das relações de solidariedade familiar, ou seja em nome do relevo pessoal e institucional dos diferentes deveres de sigilo. Tal procedimento apontará soluções diferentes de um meio de investigação para outro, de modo em que em alguns casos poderá levar em causa a omissão pura e simples do recurso ao meio de investigação, enquanto em outros poderá impor a sua imediata interrupção e ainda a destruição dos dados recolhidos que atinjam a área tutelada aqui. Em última instância, restará sempre a irredutível e inultrapassável *proibição de valoração* das manifestações que dizem respeito ao núcleo intangível da vida privada e da intimidade dos visados e de terceiros que se relaciona.[329]

Mas pela natureza das coisas, e tendo em vista que os meios ocultos de investigação são na sua maioria integrados por procedimentos automatizados, em um primeiro momento será difícil, ou até mesmo impossível, assegurar a tutela da área nuclear da intimidade logo no momento da recolha de dados ou de produção de prova. Isso só poderá ocorrer em um segundo e ulterior momento de exame e apreciação dos dados recolhidos, ou até mesmo na 25º hora, em sede de *proibição de valoração.* Assim, se se verificar que se recolheram dados atinentes a área nuclear da reserva, esses dados devem ser imediatamente destruídos, estando também definitivamente precludida a admissibilidade da sua valoração.[330]

Por outro lado, cabe aos investigadores um cuidado especial também com os *conhecimentos fortuitos* advindos das investigações criminais em ambiente digital. Atualmente, os computadores de uso pessoal têm em média 500GB e 1TB de espaço de armazenamento no disco rígido, constando nesse espaço a mais variada forma de informação pessoal do visado como de terceiros, como fotografias, vídeos, documentos

[329] *Idem,* p. 116-117.
[330] *Idem,* p. 117.

escritos (incluindo diários íntimos), registros de *websites* visitados, registros de conversas privadas, e-mails, contatos, livros, músicas e outros elementos guardados ao longo de anos de atividade perante o sistema informático, que permitem conhecer profundamente a vida e a personalidade do utilizador. Por isso é possível afirmar que a apreensão ou o acesso remoto (via *malware*, por exemplo) de um sistema informático representa o acesso a uma fonte de informação muitíssimo superior a qualquer outra acessível em processo penal. Pois, por exemplo, uma interceptação telefônica captura apenas a informação proferida no presente, e sempre em forma de uma comunicação com outrem, nunca uma manifestação dos pensamentos e sentimentos do visado, como ocorrerá se vier a ser apreendido o diário íntimo digital do mesmo via *malware*; a apreensão de correspondência limita-se aos documentos que cabem em um envelope ou aos objetos enviados em uma encomenda; uma busca, ainda que domiciliária, permite a apreensão de documentos íntimos do visado, mas estará limitada ao espaço físico da casa. Já uma pesquisa informática, diretamente no sistema ou por via remota, pode permitir o acesso a arquivos, muitas vezes estruturados pelo utilizador, de vários anos da sua vida, suscetíveis de revelaram o mais íntimo do seu ser, incluindo o histórico de relações pessoais, o conteúdo de comunicações intimas, as viagens, compras e vendas realizadas, saldos bancários, preferências e gostos secretos, etc.[331]

A tudo isso se acresce o fato de que em uma apreensão em ambiente físico sempre é necessário analisar ou visualizar os documentos e objetos apreendidos, enquanto que em uma apreensão de documentos informáticos é possível recorrer a termos de pesquisa que permitem fazer uma triagem preliminar dos documentos visados, criando assim, na pratica, um verdadeiro motor de busca da vida do visado. No que se refere à *apreensão de dados informáticos*, como já referido quando tratado sobre a pesquisa informática e a injunção para apresentação ou concessão do acesso a dados, ela geralmente é efetuada a partir de uma cópia integral do sistema informático, caso em que o visado estará frequentemente ciente da sua realização, ou a partir de uma pesquisa de dados armazenados em servidores de terceiros (como nos casos de *cloud computing*). Em ambos os casos, a informação recolhida e sujeita ao procedimento forense poderá ser analisada e explorada na integra, sem particulares restrições temporais e se necessário for, por uma pluralidade de especialistas, até a seleção final da informação com relevo probatório.[332]

[331] RAMALHO, David Silva. 2017, p. 251-252.
[332] *Ibem*, p. 253.

Assim, inexistindo vinculação temática nesta fase do processo, e sendo a pesquisa informática e a injunção, meios de obtenção de prova que não estão sujeitos á precedência da verificação de crimes de catálogo, há elevados riscos de a investigação se transformar em uma *fishing expedition* ou de implicar na imputação injustificada de ilícitos completamente distintos dos quais motivaram inicialmente a investigação. Ou seja, pode ocorrer que no decurso de uma *pesquisa informática* na investigação de um crime de homicídio, se conclua pela inexistência de supedâneo probatório no sistema informático pesquisado para imputar o ilícito sob investigação ao arguido, mas por outro lado, poderá se concluir que o visado deverá responder, em processo novo a instaurar, pela prática de um crime de ofensa á honra do Presidente da República (art. 328°, n° 1, do CP), por ter sido encontrado no seu sistema informático um e-mail enviado a um conhecido seu onde continham ofensas à honra do Chefe de Estado, ou mesmo por ter publicado essas afirmações de maneira anônima na Internet, ao abrigo do n° 2 do mesmo preceito.[333]

Nessa linha, David Silva Ramalho muito bem refere que "não é pelo facto de inexistir *vinculação* temática até á dedução de acusação que a investigação deixa de ter uma *orientação* temática, no mínimo delimitada, no plano dos factos, pela notícia do crime. O que, naturalmente, não obsta a que, se, no decurso da investigação orientada tematicamente, se encontrarem *fortuitamente* elementos probatórios da prática de outro tipo de ilícito, não possam os mesmos ser utilizados no mesmo ou noutro processo criminal a instaurar. Na medida em que o meio em causa não careça da verificação prévia de um crime de catálogo, é essa a solução pacífica".[334]

Mas como concluiu o autor, a disponibilidade de uma fonte quase "inesgotável" de informação e a disponibilidade de ferramentas técnicas capazes de analisar toda essa informação não deve legitimar a sua análise indiscriminada em buscas de novas *notitiae criminis* e de suporte da prática de *um qualquer crime* ao invés da procura de prova dos crimes sob investigação.[335]

Por outro lado, nos casos de meios de obtenção de prova sujeitos a crimes de catálogo (como é o caso dos métodos ocultos), a resposta não será a mesma e muito menos tão simples, onde deverá recorrer-se ao critério de "ponderação vinculada" previamente realizado pelo legislador na determinação dos ilícitos que justificam

[333] *Idem*, p. 253-254.
[334] *Idem*, p. 254.
[335] *Ibidem.*

semelhante grau de intromissão e, por aplicação direta, por remissão ou analogia, será aplicada a regra dos conhecimentos fortuitos prevista no art. 187°, n° 7, do CPP. Dessa maneira, se verificada a prática de um outro ilícito de catálogo, e verificado o cumprimento dos demais pressupostos de aplicação do método através do qual foi descoberto fortuitamente o novo ilícito, recorrer-se-á ao *principio do limiar da intervenção equivalente ou da intervenção substitutiva hipotética* para legitimar a mudança de fim que justifica que o meio de obtenção de prova utilizado inicialmente para um fim possa ser agora utilizado para outro. [336]

E caso estejam em causa meios de obtenção de prova que não estão sujeitos à análise de crimes de catálogo, e, portanto aos quais não se aplica a regra dos conhecimentos fortuitos, a solução, como já referido, não deverá ser a da total liberdade de pesquisa e valoração de toda informação com caráter probatório criminal contido no sistema informático. Se fosse assim, seria permitida uma busca em todo o sistema informático por meses, em busca de quaisquer provas de quaisquer ilícitos, e tendo em vista o caráter altamente invasivo do acesso ao sistema informático do visado, atingindo de maneira especialmente grave os direitos fundamentais do mesmo, devem ser determinados certos limites de acordo com o princípio da proporcionalidade. Disso, desdobra-se a importância de um registro exaustivo e constante de todos os passos da recolha, exame e análise da prova digital, incluindo os termos de pesquisas empregados. Assim, caso seja constatado que foram utilizados termos de pesquisa excessivamente amplos que resultaram na prova recolhida, bem como o emprego de procedimentos estranhos que vão além daqueles que permitiriam obter resultados uteis para a investigação, deverá concluir-se pela proibição de valoração dessa prova, tendo em vista a ingerência excessiva e não autorizada nos direitos fundamentais e na vida privada do visado.[337]

Ademais, esse registro exaustivo e constante de todos os passos da recolha, exame e análise da prova digital, transformando-se em um verdadeiro relatório pericial contendo as opções tomadas na condução da investigação, se mostra importante também para o momento após a fase de inquérito, já em sede de julgamento, pois ao visado deve ser ofertada a possibilidade de, após o termino da medida, ter conhecimento da mesma e das informações por ela colhidas, bem como da duração e do tipo de medida que foi

[336] *Idem*, p. 255. No mesmo sentido: ANDRADE, Manuel da Costa. "O regime dos "conhecimentos de investigação" em processo penal", Revista de Legislação e Jurisprudência, Coimbra, Ano 142, n° 3981 (julho-agosto de 2013), p. 355.
[337] RAMALHO, David Silva, 2017, p. 256.

utilizada para obter prova contra si, tendo acesso ao referido relatório pericial. A obrigatoriedade de tais informações constarem nos autos se dá, pois tendo em vista a natureza dos métodos ocultos onde está excluído o contraditório em sede de inquérito, e tratando-se de uma atividade instrutória intrusiva, na falta dessas informações poderá haver violação intolerável das garantias de ampla defesa do arguido e do seu direito ao contraditório, previstos no art. 32º, nº 1 e 5, da Constituição da República Portuguesa.[338]

Ainda, tratando-se de prova digital, a sua volatilidade e fragilidade impõem requisitos de verificação de fidedignidade e de garantia da cadeia de custódia, que podem não existir mesmo com a prova obtida pelo *malware*. Como se viu, poderemos estar diante de uma prova contaminada pelos referidos ataques contra perícias forenses ou perante um sistema informático infetado com outro tipo de *malware* que permite a um terceiro controlar o sistema informático e incriminar o visado. Assim, antes mesmo da prova ser analisada pelo arguido, deverá passar por uma sindicância realizada por peritos, que deverão verificar a fidedignidade e cadeia de custódia da mesma.[339]

Portanto, na observância pelo legislador e pelo aplicador do direito dos pressupostos apresentados até aqui, acreditamos que o uso de métodos ocultos para obtenção de prova em ambiente digital (seja o agente encoberto, o uso de *malware*, ou outras medidas) estaria previsto de uma maneira suficiente e adequada, em consonância com os princípios constitucionais e processuais de um Estado Democrático de Direito, legitimando-se sua utilização no processo penal português.

Contudo, importante ter em mente que a regulação de tais medidas de forma unilateral por parte apenas de alguns países não soluciona o problema de uma forma geral, tendo em vista as características que derivam da dimensão internacional da ciberdelinquência. Realizar buscas online em um equipamento informático constituiria uma atuação com efeitos extraterritoriais se o equipamento se encontrar fora da jurisdição do Estado ordenante. Dito em outras palavras, a adoção de medidas nacionais unilaterais resulta inútil para fazer frente a uma ameaça internacional que não conhece fronteiras, e pode resultar contraproducente para os legítimos fins da investigação criminal, já que uma busca online legalmente regulada em um Estado pode ser constitutiva de um delito de intrusão informática em outro.[340] É nesse sentido que se entende pela necessidade de uma regulação transnacional e comum para as matérias

[338] RAMALHO, David Silva, 2013, p. 236.
[339] *Idem*, p. 235.
[340] PRADILLO, Juan Carlos Ortiz. 2011, p. 77.

envolvendo a ciberdelinquência e a obtenção de provas em ambiente digital, e que seja mais densa e clara do que as já existentes (como a Convenção de Budapeste sobre o Cibercrime), principalmente quando se está diante de métodos ocultos de investigação com alcances extraterritoriais.

# CONCLUSÃO

Por todo o exposto aqui, consideramos que a melhor resposta que pode ser dada em um Estado de Direito aos novos desafios que a aplicação da informática gera para as investigações criminais é uma reforma do Direito Processual Penal, prevendo os métodos de investigação criminal em ambiente digital de uma maneira suficiente para garantir o respeito aos princípios da legalidade, segurança jurídica, claridade e proporcionalidade, e permitindo as autoridades judicias e policiais do Estado servir-se de um modo eficaz dos avanços tecnológicos e das dificuldades da persecução criminal na era digital.

Essa exigência se agrava quando estamos diante de métodos ocultos de investigação como os tratados aqui, tendo em vista a enorme ingerência e especial gravidade que o emprego de tais medidas representam para os direitos fundamentais, não sendo possível uma aplicação analógica da regulação estabelecida para outras medidas de investigação que podem conter certas relações e semelhanças, ainda mais quando se busca adaptar um método de investigação previsto para o ambiente físico no ambiente digital, tendo em vista as enormes diferenças existentes entre ambos os mundos.

E por mais que as lacunas e carências de regulação legal possam ser complementadas pela interpretação do aplicador do direito, tais interpretações não podem suprir a necessidade de uma *lex stricta y lex praevia*, principalmente quando se está diante de medidas de investigação limitativas de direitos fundamentais. Porém, se mostra uma tarefa muito difícil para o legislador regular taxativamente todas as medidas e consequências legais relacionadas com a tecnologia, tendo em vista sua constante evolução, possibilitando a todo instante novos meios de investigação.

É em razão disso que deve ser previsto uma teoria geral dos métodos ocultos de investigação (seja em ambiente físico ou digital), respeitando todos os requisitos elencados anteriormente e que servirão de coordenada para o aplicador do direito na análise do caso concreto. Assim, seguindo tais coordenadas, o trabalho do legislador para prever novos métodos ocultos ficará mais simples e eficiente, facilitando a tarefa de acompanhar a evolução tecnológica e a criação de novos métodos ocultos de investigação em ambiente digital.

Portanto, entendemos que uma previsão adequada e unificada dos métodos ocultos de investigação, aliada com as devidas reformas na matéria sobre a obtenção de provas em ambiente digital, como a previsão expressa e clara da utilização de *malware* (buscas online), seriam fortes armas para o Estado combater a criminalidade mais grave, como o crime organizado e o terrorismo, tendo em vista que hoje os sistemas informáticos representam uma fonte de provas dos mais variados ilícitos, necessitando de meios de investigação adequados para que os criminosos não se aproveitem da sombra do anonimato e da impunidade.

O que não se pode é abrir mão da modernização e da utilização de meios de obtenção de prova tão eficientes como o *malware* e o agente encoberto em ambiente digital, enquanto que da mesma forma não se pode admitir sua utilização sem uma previsão legal expressa, que garanta que a restrição de direitos fundamentais se dê de uma maneira proporcional, alcançando assim o equilibro entre segurança pública e os direitos fundamentais dos investigados.

# BIBLIOGRAFIA


ALBRECHT, Hans-Jorg. *"Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos*, em AA.VV, Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português, Coimbra: Coimbra Editora, 2009.

ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 4º edição, Universidade Católica Portuguesa, Lisboa, 2011.

ANDRADE, Manuel da Costa. Sobre as Proibições de Prova em Processo Penal¸ Coimbra: Coimbra Editora, 1992.

ANDRADE, Manuel da Costa, Métodos ocultos de investigação (Pladoyer para uma teoria geral), in: Gelson Bonato (org.) Processo Penal, Constituição e Crítica - Estudos em homenagem ao Prof. Dr. Jacinto Nelson de Miranda Coutinho, Rio de Janeiro: Lumen Juris, 2011, p. 525-551.

ANDRADE, Manuel da Costa. "*Bruscamente no Verão Passado", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia ter sido diferente*, Coimbra: Coimbra Editora, 2009.

ANDRADE, Manuel da Costa. "O regime dos "conhecimentos de investigação" em processo penal", Revista de Legislação e Jurisprudência, Coimbra, Ano 142, n° 3981 (julho-agosto de 2013), p. 352-377.

BERINATO, Scoot. *The Rise of Anti-Forensics*, CSO Online, 2007. Disponível em: http://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html.

BETTINI, Claudio/ JAJODIA, Sushil/ SAMARATI, Pierangela/ WANG, Sean X., *Privacy in Location-Based Applications: Research Issues and Emerging Trends*, Berlim/Heidebelg/ Nova Iorque: Springer, 2009.

BLAKESLEE, Melise R., *Internet Crimes, Torts and Scams – Investigation and Remedies*, Oxford: Oxford University Press, 2010.

BOLDT, Martin. *Privacy-Invasive Software*, Karlskrona: Blekinge Institute of Technology, 2010. Disponível em: http://www.bth.se/tek/aps/mbo.nsf/bilagor/boldt_thesis_v1_02_pdf/$file/boldt_thesis_v1.02.pdf.

CABRAL, José Santos. "Anotação ao artigo 126º - Métodos proibidos de prova", Código de Processo penal comentando, Coimbra: Almedina, 2014.

CANOTILHO, J. J Gomes e MOREIRA, Vital. Constituição da República Portuguesa Anotada, Vol. I, 4.ª ed., Coimbra: Coimbra Editora, 2007.

CONDE, Francisco Muñoz. *De nuevo sobre el derecho penal del enemigo,* 2ª ed., Buenos Aires: Hammurabi, 2007.

CONDE, Francisco Munõz. *La búsqueda de la verdade en el processo penal*, Buenos Aires: Hammurabi, 2007.

COLE, Eric. *Hiding in plainsight: Steganography and the Art of Covert Communication*, Indiana: Wiley Publishing, 2003.

CORREIRA, João Conde. Contributo para a análise da inexistência e das nulidades processuais, Coimbra: Coimbra Editora, 1999.

CORRERIA, João Conde. "Questões práticas relativas á utilização de diários íntimos como meio de prova em processo penal", em Revista do CEJ, nº 6 (1º semestre de 2007), p. 139-160.

CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter, in: Revista do Ministério Público, ano 35, nº 139, Lisboa, 2014, p. 29-59.

COSTA, Eduardo Maia. "*Ações encobertas (Alguns problemas, algumas sugestões*)", em AA.VV., Estudos em Memória do Conselheiro Artur Maurício, Coimbra: Coimbra editora, 2014.

CRIADO, Miguel Ángel Poveda. *Delitos en la Red: Cibercrimen, Ciberdelitos, Ciberseguridad, Ciberespionaje y Ciberterrorismo*, Madrid: Editora Fragua, 2015.

CURRAN, Kevin/ BRESLIN, Peter/ MCLAUGHLIN, Kevin/ TRACEY, Gary. *Hacking and Eavesdropping*, em *Cyber Warfare and Cyber Terrorism* (orgs. Lech J. Janczewski e Andrew M. Colarik), Nova Iorque: Information Science Reference, 2008, p. 307-317.

DA SILVEIRA, Maria Ana Barroso de Moura. *Da problemática da investigação criminal em ambiente digital - em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova*, Dissertação de Mestrado orientada pelo Professor Doutor Germano Marques da Silva, Universidade Católica Portuguesa: Lisboa, 2016.

DIAS, Jorge de Figueiredo. "*Direito à informação, protecção da intimidade e autoridades administrativas independentes*", Estudos em Homenagem ao Professor Doutor Sérgio Soares, Coimbra: Coimbra Editora, 2001.

DIAS, Jorge de Figueiredo. O processo penal português: problemas e perspectivas, in AA.VV, Que futuro para o direito processual penal? – Simpósio em homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal português, Coimbra: Editora Coimbra, 2009.

DIAS, Jorge de Figueiredo. "Por onde vai o Processo Penal Português – por estradas ou por veredas?", em *As conferência do Centro de Estudos Judiciários,* Coimbra: Almedina, 2014.

DOMÍNGUES, Francisco Lázaro. *Introducción a la informática Forense,* Madrid: Ra-Ma, 2013.

FILIOL, Eric. *Computer viruses: from theory to applications,* França: Springer, 2005.

FROSINI, Vittorio. *Informática y Derecho,* Bogotá: Editorial Temis, 1988.

FURTADO, Franklim. "*O agente infiltrado",* Direito e Cidadania, Ano V, nº 16/17 (setembro de 2002/abril de 2003).

GONÇALVES, Fernando/ ALVES, Manuel João/ VALENTE, Manuel Guedes. O novo regime jurídico do agente infiltrado (Comentado e Anotado – Legislação complementar), Coimbra: Almedina, 2001.

GOSSEL, Karl Heinz. *El Derecho Processal Penal en el estado de Derecho,* Buenos Aires: Rubinzal – Culzoni Editores, 2007.

GRINOVER, Ada Pellegrini/ FERNANDES, Antônio Scarance/ GOMES FILHO, Antônio Magalhães. As nulidades no processo penal, 2ª ed., São Paulo: Malheiros, 2000.

HARRIS, Ryan. *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensic sproblem, Digital Investigation - The international Journal of Digital Forensics & Incident Response,* Vol. 03 – Suplemento, 2006.

HASSEMER, Winfried. *Fundamentos del derecho penal,* trad. de Arroyo Zapatero y Muñoz Conde, Barcelona: Bosch, 1984.

JACOBY, Nicole. "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality Of Technical Surveillance Measures in Germany and the United States", em *Georgia Journal of International and Comparative Law,* vol. 35, n° 3, 2007.

JAGER, Christian. *Problemas fundamentales de derecho penal y procesal penal,* Buenos Aires: Fabian J. Di Placido, 2003.

JAKOBS, Gunther e MELIÁ, Manuel Cancio. Direito Penal do Inimigo: noções e criticas, org. e trad. André Luis Callegari, Nereu José Giacomolli, 2ª ed., Porto Alegre: Livraria do Advogado, 2007.

KERR, Orin S., "*The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?*", 33 *Connecticut Law Review 503,* Vol. 33, 2001. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=927973.

KERR, Orin S., "*Digital evidence and the new Criminal Procedure",* Columbia Law Review, Vol. 105, n° 1 (Janeiro de 2005), p. 281-289.

MATA-MOUROS, Maria de Fátima. Juiz das Liberdades – Desconstrução de um Mito do Processo Penal, Coimbra: Almedina, 2011.

MEIREIS, Manuel Alves. O regime das Provas Obtidas pelo Agente Provocador em Processo Penal, Coimbra: Almedina, 1999.

MENDES, Paulo de Sousa, Lições de Direito Processual Penal, Coimbra: Almedina, 2013.

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

MILLER, Arthur R. *The Assault on Privacy*, Michigan: University of Michigan Press, 1970.

NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer electronic cash system,* 2008. Disponível em: https://bitcoin.org/bitcoin.pdf.

NEVES, Rita Castanheira. As ingerências nas comunicações electrônicas em processo penal, Coimbra: Coimbra Editora, 2011.

NOVAIS, Jorge Reis. Os princípios constitucionais estruturantes da República Portuguesa, Coimbra: Coimbra Editora, 2004.

NUÑEZ, Eloy Velasco. *Delitos cometidos a través de Internet. Cuestiones procesales,* Madrid: La Ley, 2010.

NUÑEZ, Eloy Velasco. *ADSL y Troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal*, La Ley Penal, nº 82, 2011, p. 18-25.

PEREIRA, Rui. "*O "agente encoberto" na ordem jurídica portuguesa*", em AA.VV., Medidas de Combate á Criminalidade Organizada e Econômico-Financeiro, Coimbra: Coimbra Editora, 2004.

PÉREZ-LUNO, Enrique. *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 2005.

PINTO, Lara Sofia. "Privilégio contra a auto-incriminação versus colaboração do arguido. *Case study:* revelação da *password* para desencriptação de dados – *resistance is futile?*", em Prova Criminal e Direito de Defesa. Estudos sobre Teoria da Prova e Garantias de Defesa em Processo Penal (coord. Teresa Pizarro Beleza/Frederico de Larcerda da Costa Pinto), Coimbra: Almedina, p. 91-116, 2013.

PRADILLO, Juan Carlos Ortiz, *Problemas procesales de La Ciberdelincuencia,* Madrid: Editorial Colex, 2009.

PRADILLO, Juan Carlos Ortiz, *Remote Forensic Software as a Tool for Investigating Cases of Terrorism, ENAC – E-newsletter on the fight againt cybercrime, nº 4,* 2009, p. 1-8. Disponível em: *http://polis.osce.org/library/f/3643/2779/NGO-ESP-RPT-3643-EN-2779.pdf.*

PRADILLO, Juan Carlos Ortiz. *Hacking'legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquencia informática,* Revista Aranzadi de Derecho y Processo Penal, n° 26, 2011-2, Navarra: Thomson Reuters Aranzadi, 2011.

PRADILLO, Juan Carlos Ortiz. "*Informática y derechos fundamentales: hacia un derecho fundamental a la confidencialidad e integridad de los equipos informáticos",* em *El derecho en la sociedad telemática: estudios en homenaje a Valentín Carrascosa López,* (coord. Marcelo Bauzá Reilly, Federico Bueno de Mata), Santiago de Compostela: Andavira Editora, 2012.

PRADILLO, Juan Carlos Ortiz, *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, 2013. Disponível em: http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf.

PRADILLO, Juan Carlos Ortiz. "*El impacto de la tecnología en la investigación penal y en los derechos fundamentales",* em VV.AA. *Problemas actuales de la justicia penal*, Madrid: Ed. Colex, 2013.

RAMALHO, David Silva. O uso de *malware* como meio de obtenção de prova em processo penal, in Revista de concorrência e regulação, Lisboa, Ano 4, nº 16, 2013, p. 195-243.

RAMALHO, David Silva. A recolha da prova em sistemas de computação em nuvem. In Revista de direito intelectual, Nº 2, Coimbra, 2014, p. 123-162.

RAMALHO, David Silva. *Métodos ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017.

RIBOLI, Eduardo Bolsoni. "A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem", in Galileu – Revista de direito e economia, Volume XIX, Lisboa, 2018, p. 49-77.

RODRIGUES, Benjamim Silva. Das escutas telefônicas à obtenção da prova em ambiente digital. 2ª Edição revisada, atualizada e aumentada, Coimbra: Editora Coimbra, 2009.

ROWLAND, Diane/ KOHL, Uta/ CHARLESWORTH, Andrew. *Information Technology Law,* 4.ª Ed. Nova Iorque: Routledge, 2012.

ROXIN, Claus. *"La protección de la persona en el derecho processal alemán",* em *La evolución de la política criminal, el derecho penal y el proceso penal*, Valencia: Tirantlo Blanch, 2000.

ROXIN, Claux. *La prohibición de autoincrinación y de las escuchas domiciliares*,apresentação de Francisco Muñoz Conde e Marcela De Langhe, Buenos Aires: Hammurabi, 2008.

SANTOS, Osvaldo. *Firewalls – Soluções práticas,* Lisboa: FCA – Editora de Informática, 2011.

SILVA, Germano Marques da. *Bufos, infiltrados, provocadores e arrependidos,* in Direito e Justiça, F.D.U. Católica, vol VIII, T. 2, 1994.

SINROD, Eric J. e REILLY, William P., *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws,* Santa Clara Computer and High Technology Law Journal, Vol. 16, nº 2, 2000.

SCHAFER, Burkhard e MASON, Stephen. "*The characteristics of electronic evidence in digital format*", em AA.VV., *Eletronic Evidente(*Stephen Maison*),* Londres: Lexis Nexis Butterwoths, 2012

SOLOVE, Daniel J. *Conceptualizing Privacy*. California: California Law Review, 2002. Disponível em:http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview.

SOUSA, Susana Aires de. "*Agent provocateur e meios enganosos de prova. Algumas reflexões",* em AA.VV, Liberdiscipulorum para Jorge de Figueiredo Dias (org. Manuel da Costa Andrade *et al.),* Coimbra: Coimbra Editora, 2003.

SYLSVESTRE, Fabio Zech e LIMA, Pedro Souza. O direito fundamental á privacidade em face da administração pública, 2012. Disponível em: http://editora.unoesc.edu.br/index.php/simposiointernacionaldedireito/article/view/1586/1041.

VACCA, John R., *Computer Forensics, Computer Crime Scene Investigation.* Charles River Media, Inc., Hingham, Massachusetts, 2002.

VENÂNCIO, Pedro Dias, Lei do Cibercrime – Anotada e comentada, Coimbra: Coimbra editora, 1º edição, 2011.

VERDELHO, Pedro. "Lei do Cibercrime", em AA.VV., *Enciclopédia de Direito e Segurança* (coord. Jorge Bacelar Gouveia e Sofia Santos), Coimbra: Almedina, 2015.

VIGNA, Paul e CASEY, Michael J., *The age of Cryptocurrency – How Bitcoin and Digital Money are challenging the Global Economic Order*, Nova Iorque: St. Martin's Press, 2015.

WARREN, Samuel D. e BRANDEIS, Louis D. *The Right to Privacy*, Harvard Law Review, Vol. 4, Nº 5, 1898. Disponível em: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

WEBER, Rolph e HEINRICH, Ulrike I., *Anonymization*, Londres: Springer, 2012.

## JURISPRUDÊNCIA

TRIBUNAL Constitucional Federal – Acórdão da Primeira Sala de n.º 370/07 e 595/07, de 27 de fevereiro de 2008 [Em linha], [Consult. 4 Jan. 2018], disponível em < http://www.bverfg.de/e/rs20080227_1bvr037007.html >.

TRIBUNAL Constitucional Federal – Acórdão da Primeira Sala de n.º 19/63, de 16 de julho de 1969.

SUPREMO Tribunal de Justiça – Acórdão com o n.º 886/07.8PSLSB.L1.S1, de 3 de março de 2010, Relator: Santos Cabral.

SUPREMO Tribunal de Justiça – Acórdão com o n.º 06P2321, de 20 de Setembro de 2009, Relator: Armindo Monteiro.

TRIBUNAL Constitucional – Acórdão de n.º 593/03, de 5 de dezembro de 2003, Relator: Benjamim Rodrigues

TRIBUNAL Constitucional – Acórdão de n.º 835/98, de 14 de outubro de 1998, Relator: Messias Bento.

TRIBUNAL da Relação de Évora – Acórdão de n.º 238/12.8PBPTG.E1, de 19 de Maio de 2015, Relator: António Latas.

TRIBUNAL da Relação de Lisboa – Acórdão de n.º 189/09.3JASTBL.L1-5, de 30 de Junho de 2011, Relatora: Filomena Lima.

TRIBUNAL da Relação de Lisboa – Acórdão de n.º 1695/09.5PJLSB.L1-9, de 19 de junho de 2014, Relatora: Margarida Vieira de Almeida.

TRIBUNAL da Relação do Porto – Acórdão de n.º 585/11.6PAOVR.P1, de 24 de Abril de 2013, Relatora: Fátima Furtado.