UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

HELDER AUGUSTO RODRIGUES GOMES

PESQUISAS INFORMÁTICAS EM FRONTEIRAS DIGITAIS: JURISDIÇÃO E USO DE *MALWARE* PELAS FORÇAS POLICIAIS

Dissertação de Mestrado em Direito e Prática Jurídica

Especialidade de Direito Penal

Orientador

Professor Doutor Paulo de Sousa Mendes

LISBOA, 2025

UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

HELDER AUGUSTO RODRIGUES GOMES

PESQUISAS INFORMÁTICAS EM FRONTEIRAS DIGITAIS: JURISDIÇÃO E USO DE *MALWARE* PELAS FORÇAS POLICIAIS

Dissertação de Mestrado em Direito e Prática Jurídica

Especialidade de Direito Penal

Orientador

Professor Doutor Paulo de Sousa Mendes

LISBOA, 2025

Agradecimentos

Aos meus Pais, Aníbal e Maria, na essência, por tudo o que sou.

À minha mulher Isabel e meu filho Daniel por tudo, que tem sido, seguramente, bem mais do que tenho dado.

"Here" is "nowhere".

Pedro Verdelho, "*Obtaining digital evidence in the global world*", UNIO - EU Law Journal. Vol. 5, No. 2, July 2019, pp 136-145.

Resumo

Neste trabalho analisamos os desafios legais impostos pelas investigações e pesquisas informáticas transfronteiriças, principalmente aquelas em que através da utilização de meios tecnológicos e técnicas antiforenses, os criminosos dificultam não só a sua identificação, mas também a recolha de prova que os possa incriminar. No âmbito dessas pesquisas informáticas analisaremos se o nosso ordenamento jurídico permite a utilização, por parte das forças policiais, de técnicas e meios ocultos de investigação, nomeadamente, o *malware* por parte de agentes encobertos informáticos. Transpostas que sejam as fronteiras digitais, veremos como é que a nível internacional e, em particular na União Europeia, se previne e regula os conflitos de jurisdição e como está regulada a cooperação judiciária internacional.

Palavras-chave: Prova digital, pesquisas informáticas transfronteiriças, jurisdição, agente encoberto informático, *malware*.

Abstract:

In this paper, we analyze the legal challenges posed by cross-border computer investigations and searches, especially in those situations in which, through the use of technological means and anti-forensic techniques, crime agent make it difficult not only to identify them, but also to collect evidence that could incriminate them. In the context of these computer searches, we will analyze whether our legal system allows the use, by police forces, of hidden investigation techniques and means, namely malware, by undercover computer agents. Once digital borders have been crossed, we will see how at an international level, and in particular in the European Union, disputes are prevented and regulated, and how international judicial cooperation is regulated.

Keywords: Digital evidence, cross-border computer searches, jurisdiction, cyber undercover agent, malware,

Abreviaturas, siglas e acrónimos

Ac.	Acórdão
AcE	Ações encobertas
AE	Agente encoberto
AJ	Autoridade Judiciária
CAAS	Convenção de Aplicação do Acordo Schengen
CBCc	Convenção Cibercrime
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CCiber	Convenção sobre o Cibercrime
CE	Comissão Europeia
cit.	Obra citada
CoE	Conselho da Europa
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
DEFR	*Digital Evidence First Responder*
DES	*Digital Evidence Specialist*
DG JUST	*Directorate-General for Justice AND Consumers*
ed.	Edição
EDES	*Evidence Digital Exchange System*
EM	Estado Membro
EPPO	*European Public Prosecutor´s Office*
FBI	*Federal Bureau of Investigation*
FRCP	*Federal Rules of Criminal Procedure*
i.e.	Locução que significa isto é
IOCE	*International Organization on Computer Evidence*
IP	*Internet Protocol*
JIC	Juiz de Instrução Criminal
JOUE	Jornal Oficial da União Europeia
LCc	Lei do Cibercrime
LECrim	*Ley de Enjuiciamiento Criminal*

MD5	*Message-Digest Algorithm 5*
MP	Ministério Público
NHS	*Nacional Health Care*
NIT	*Network Investigative Technique*
ONU	Organização das Nações Unidas
OPC	Orgão de Polícia Criminal
PE	Parlamento Europeu
PJ	Polícia Judiciária
RASI	Relatório Anual de Segurança Interna
RGPD	Regulamento Geral de Proteção de Dados
RIC	Redes de Informação e Comunicação
RJAE	Regime Jurídico das Ações Encobertas
SHA	*Secure Hash Algorithm*
STJ	Supremo Tribunal de Justiça
SWGDE	*Scientific Working Group on Digital Evidence*
T-CY	Comité da Convenção Cibercrime
TEDH	Tribunal Europeu dos Direitos Humanos
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
USB	*Universal Serial Bus*
v.g.	*Verbi gratia* (locução latina que significa "pela graça da palavra" e equivale a "como tal" e "por exemplo"
VPN	*Virtual Private Network*
Wi-Fi	*Wireless Fidelity*

Índice

INTRODUÇÃO

As tecnologias de informação têm tido um impacto enorme nas sociedades modernas, acelerando a mudança tecnológica em vários setores. Trouxe benefícios para a economia e para a sociedade, mudando os nossos hábitos sociais, profissionais e de relacionamento com empresas e organismos públicos.

Apesar destes benefícios, infelizmente, as tecnologias de informação também têm sido usadas por indivíduos e grupos criminosos que, aproveitando-se das fragilidades dos utilizadores e sistemas, cometem crimes cada vez mais sofisticados. Com conhecimentos próprios e por vezes mediante o auxílio de especialistas informáticos, conseguem, invariavelmente, ficar no anonimato e furtar-se ao sistema de justiça.

Perante fenómenos criminais graves, devido à volatilidade das provas digitais, espera-se por parte das autoridades judiciárias e órgãos de polícia criminal (OPC), uma atuação célere com vista a assegurar a identificação dos agentes criminosos bem como a obtenção e apreensão de prova relevante, inviabilizando a impunidade destas condutas. Não obstante, por vezes estes deparam-se com dificuldades de localização física dos agentes, da infraestrutura criminosa ou da própria localização da prova digital (*Loss of Location*), sendo que, para complicar um pouco a encruzilhada, os três até podem estar separados em Estados diferentes.

Decidindo-se pelo avanço unilateral das pesquisas informáticas são inúmeros os problemas que podem vir a surgir. Abordaremos dois. O primeiro diz respeito à delimitação da jurisdição competente para proceder à investigação, na medida em que se por um lado os efeitos do crime se fazem sentir no Estado que leva a cabo a investigação, por outro lado, o agente criminoso, os meios por este utilizados, ou a própria localização da prova digital são totalmente desconhecidos. Ora, esta situação pode ocasionar conflitos jurisdicionais. Assentando os poderes de investigação criminal no princípio da territorialidade e jurisdição das autoridades, veremos quais as medidas e ferramentas que existem para a resolução deste problema, principalmente, a nível europeu, analisando a forma como o *European Public Prosecutors Office* (EPPO) aborda esta questão. A respeito do nosso ordenamento jurídico, veremos como o legislador nacional optou no art.º 15.º, n.º 5, da Lei do Cibercrime, pela supressão da limitação territorial que constava do art.º 19.º da Convenção sobre o Cibercrime. Ampliou desta forma o âmbito de aplicação das pesquisas informáticas a dados armazenados, possibilitando nas investigações criminais nacionais a realização de acessos transfronteiriços, sem contudo, reconhecer qualquer reciprocidade às autoridades estrangeiras. Reconhece e protege aos

cidadãos nacionais direitos fundamentais e ao Estado, princípios de soberania. Às investigações levadas a cabo por autoridades de Estados estrangeiros impõe o recurso aos mecanismos de cooperação judiciária internacional (art.º 25.º da Lei do Cibercrime). Esta dualidade coloca em causa princípios e normas de Direito Internacional bem como direitos fundamentais dos cidadãos que enunciaremos, mas não abordaremos de forma profunda.

Importa dotar as investigações criminais de meios que permitam perseguir de forma eficaz os agentes da prática de crimes cujo suporte probatório se encontra em formato digital, salvaguardar os interesses dos Estados visados em não sofrerem ingerências diretas em sistemas informáticos localizados dentro das suas fronteiras, bem como reconhecer e salvaguardar o direito à privacidade dos cidadãos. Ora, este equilíbrio é bastante frágil.

O segundo problema acaba por ser uma decorrência do primeiro, na medida em que nos termos expostos, verifica-se também problemas na delimitação da legislação aplicável para obtenção daquela concreta prova digital, ou seja, sendo desconhecida a localização da prova também é desconhecido se nesse Estado se faz uso de técnicas e métodos de investigação ocultos, ou seja, recurso a agentes encobertos e poderes especiais de investigação (*hacking* ou monitorização de atividades criminosas). A este respeito veremos no nosso ordenamento jurídico o art.º 19.º da Lei do Cibercrime que diz respeito às ações encobertas, relativamente ao qual a doutrina se tem vindo a referir a este meio de obtenção de prova como ações encobertas em ambiente digital, que por sua vez faz uma remissão genérica para o regime da Lei n.º 101/2001, de 25 de agosto, Regime Jurídico das Ações Encobertas para fins de prevenção e investigação criminal (RJAE).

Analisaremos por fim os casos em que para efetivação da recolha de prova digital, os OPC fazem uso de um meio específico de extração de informação oculto para o(s) visado(s). Falamos, concretamente de *software* de recolha de informação (*malware*) e veremos o seu enquadramento e (in)admissibilidade no nosso ordenamento jurídico.

METODOLOGIA ADOTADA

Estruturamos esta dissertação em cinco partes: na primeira abordamos a prova digital em investigações digitais transfronteiriças onde, como linha orientadora deste estudo, começaremos por ilustrar os dois problemas com dois casos reais, um deles referido e descrito por MARGARIDA NEIVA ANTUNES[1] e que neste trabalho, sem perder a essência, procuramos resumir. Nesta parte para melhor compreensão do tema, analisaremos os conceitos de ambiente digital e prova digital, as dificuldades da sua localização (*loss of location*) bem como a importância da sua recolha de acordo com os trâmites da ciência forense digital; na segunda parte abordamos a Jurisdição competente em investigações digitais transfronteiriças, recordando conceitos de soberania, território e jurisdição e a forma como a última é aferida no *European Public Prosecutor´s Office* (EPPO). Aqui veremos o impacto das investigações informáticas transfronteiriças na soberania dos países e implicações ao nível dos conflitos jurisdicionais; na terceira parte veremos as pesquisas informáticas transfronteiriças e o respetivo enquadramento legal; na quarta parte abordamos as ações encobertas em ambiente digital, enquadramento legal e intervenientes; na quinta parte o recurso a *malware*[2] como meio de obtenção de prova e legitimidade de utilização no nosso ordenamento jurídico.

[1] ANTUNES, Margarida Neiva, *A Obtenção de Prova Digital Mediante Acessos Transfronteiriços em Contexto de Loss of Location* in *Novos Desafios da Prova Penal*, MENDES, Paulo Sousa / PEREIRA, Rui Soares (Coordenação), Vol.II, Coimbra, 2023, (pp.571-610), p.575. ISBN 978-989-40-1059-3

[2] Cf. RAMALHO, David Silva, *O Uso de Malware Como Meio de Obtenção de Prova em Processo Penal* in Revista de Concorrência e Regulação [Em linha]. Ano IV, n.º 16 (2013), 195-243, p.201. Disponível na Internet:URL:<https://catalogo.pgr.pt/cgi-bin/koha/opac-detail.pl?biblionumber=243580>, que resume a definição de *ransomware*, como todo o tipo de programas instalados sub-repticiamente por terceiros num sistema informático que podem ser utilizados para, de algum modo, comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao sistema informático infetado, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos. [Consulado em 17/05/2024].

1. A PROVA DIGITAL EM INVESTIGAÇÕES DIGITAIS TRANSFRONTEIRIÇAS

De forma incontornável a internet passou a fazer parte integrante das nossas vidas. Através dela, trabalhamos, socializamos, divertimo-nos e consumimos os mais diversos tipos de produtos e serviços. Com um simples "clique" numa qualquer página da internet, interagimos com o "outro lado do mundo".

É certo que nem todas as interações e dados gerados terão relevo probatório, no entanto, aqueles que estejam de certa forma ligados/associados à prática de crime(s), transformam-se em prova digital que urge, num primeiro momento salvaguardar e depois recolher como elemento de prova. A internet e os recursos tecnológicos que os próprios criminosos dispõem, invariavelmente, colocam entraves às autoridades judiciárias que os investigam, motivo pelo qual, devemos compreender o conceito, importância e relevância da sua recolha.

Entretanto e por forma a melhor ilustrar os problemas que suscitamos, vejamos dois casos reais no ordenamento jurídico norte-americano.

1.1 *O caso In re warrant to search a target computer at premises unknown*[3]

Em 2013, o *Federal Bureau of Investigation* (FBI) deu início a uma investigação criminal devido ao facto de desconhecido(s), ter(em) acedido indevidamente à conta de e-mail da vítima (um cidadão do Estado do Texas) e através desta, à sua conta bancária. Mediante o uso de um endereço de e-mail em tudo idêntico ao da vítima, tentaram efetuar uma transferência bancária de elevado montante, para uma conta bancária sediada no estrangeiro.

Em causa estaria a prática do crime de fraude bancária, roubo de identidade e violação de leis de segurança de informação.

Pese embora os esforços empreendidos, apesar do endereço do IP do computador utilizado apontar para que este estivesse fora do território norte-americano, os agentes do FBI nunca conseguiram determinar a localização exata dos suspeitos ou do dispositivo.

Junto do *US District Court for the Southern District of Texas* requereram a emissão de um mandado de busca e apreensão ao abrigo da *Rule 41* prevista na *Federal Rules of Criminal Procedure* (FRCP), essencial para prosseguimento da investigação.

[3] Cf. (ANTUNES, 2023, p. 575).

O objetivo seria obter autorização, por 30 dias, para instalação oculta de um *software* de extração de informação no computador utilizado na prática dos crimes, logrando desta forma obter os registos de atividade na internet, os registos de endereços de IP e indícios relativamente à identidade do detentor do computador (*hacking)*[4]. Simultaneamente, permitiria obter informação de forma prospetiva, como dados sobre novas vítimas, a captura de fotografias através da *webcam* do computador, possibilitando a identificação dos seus utilizadores, e informações sobre a localização do dispositivo.

O Estado norte-americano, embora desconhecendo a localização geográfica exata ou aproximada do computador utilizado, entendeu que a informação seria propriedade localizada dentro do próprio distrito, cumprindo a exigência da *Rule 41 (b) (1)*[5]. A fundamentar tal entendimento, referiu que a busca se realizaria mediante um acesso remoto, em que os agentes do FBI não teriam que efetuar qualquer deslocação física para obter a informação do computador alvo, além de que a respetiva análise de prova se circunscreveria ao território do distrito do Tribunal.

Não foi esse o entendimento perfilhado pelo Tribunal, sustentando que a pretensão do Estado norte-americano envolveria a realização de busca fora dos limites territoriais impostos pela norma habilitante, concluindo: "*A informação digital não está, de facto, guardada na nuvem; encontra-se num computador ou noutro dispositivo electrónico que tem uma localização física"*[6]. Afirmou que ocorrendo as buscas em dispositivo que se encontra em lugar físico indeterminado, não era possível afirmar que as mesmas se circunscreveriam aos limites territoriais do distrito, recusando a emissão do mandado com base na prerrogativa invocada pelo Estado. O desconhecimento da localização do computador alvo (e o facto de não se tratar de um caso de terrorismo) impedia também a verificação das demais alíneas da *Rule 41 (b)*, motivo pelo qual o Tribunal, na ausência de suporte legal e invocando, ainda, falta de cumprimento das exigências da 4ª Emenda e dos *standards* para a videovigilância, acabou por negar a emissão do mandado.

[4] *Hacking* refere-se à ação de identificar e explorar vulnerabilidades de um sistema de computador ou rede, geralmente para obter acesso não autorizado a dados pessoais ou organizacionais. O termo nem sempre se refere a uma atividade maliciosa, mas tem conotações principalmente negativas devido à sua associação com cibercrimes.

[5] Esta *Rule 41* estabelecia que um Juiz Distrital ou na sua falta, um Juiz Estadual do próprio Distrito, tem autoridade para emitir um mandado de busca e apreensão (a pessoas ou propriedades) localizados no Distrito – tradução nossa a partir da obra citada (ANTUNES, 2023,p. 575, nt. 10).

[6] Tradução nossa a partir do original (ANTUNES, 2023, p.576).

1.2 *United States of America v. Robert Mclamb (n.º 17-4299) de 26.10.2017*[7]

Neste caso, *Robert Mclamb* contestou uma decisão do Tribunal Distrital, que negou provimento à moção que havia interposto para recusa de admissão da recolha de prova de pornografia infantil encontrada e recuperada de um disco rígido que se encontrava em sua casa. Esta recolha de prova ocorreu no âmbito de uma investigação dirigida pelo FBI, relacionada com a prática de crimes de pornografia infantil visando um *website* na *dark web*[8] denominado "*Playpen*"[9].

Depois de receber uma informação anónima, o FBI apreendeu o servidor do "*Playpen*" e prendeu o administrador do *website*. No entanto, apesar de estar na posse do servidor, o FBI não conseguiu localizar os utilizadores do "*Playpen*", uma vez que, devido à utilização do Tor, os utilizadores que carregavam e descarregavam ficheiros de pornografia infantil permaneciam anónimos.

Foi nesta sequência e perante estas dificuldades que em fevereiro de 2015, o FBI solicitou a emissão de um mandado para implantar a *Network Investigative Technique* (NIT) para localizar os utilizadores que acediam ao *website*. A NIT é um *script*[10] de computador projetado para ultrapassar e superar as proteções de anonimato da *dark web* e proceder à recolha de informações que permitam a identificação dos computadores que acedem ao *site* "*Playpen*". Este *script* corrompe o servidor alvo e de forma complementar e sub-repticiamente os dados de pornografia infantil alocados com esse *script*. Depois de um utilizador aceder ao *website* e realizar determinadas ações, incluindo descarregar

---

[7] Disponível na internet:<URL:https://law.justia.com/cases/federal/appellate-courts/ca4/17-4299/17-4299-2018-01-25.html>. [Consultado em 21/04/2025].

[8] O *Onion Router* (Tor) é uma das várias redes *online* criptografadas que compõem a *dark web*. O Tor utiliza uma série de computadores de retransmissão para ocultar a identidade dos utilizadores *online*. Como resultado, o Tor anonimiza a forma como, quando e onde os utilizadores acedem à internet. Com estas poderosas e fortes proteções de anonimato e privacidade, alguns utilizam o Tor para a prática de crimes, tais como, tráfico de drogas, pornografia infantil e outros propósitos criminosos – tradução nossa a partir do texto da decisão do caso exposto.

[9] "*Playpen*" era um fórum na *dark web* onde utilizadores podiam fazer *upload* ou *download* de pornografia infantil. A determinado momento, contou com mais de 158.000 membros e quase 100.000 partilhas. Para aceder a *sites* de serviços ocultos como o "*Playpen*", um utilizador necessita num primeiro momento de instalar a rede Tor e inserir o nome de domínio do *site*, que era uma URL de 16 caracteres composta por letras e números aleatórios. O "*Playpen*" não era disponibilizado na internet aberta nem tão pouco os motores de busca como o Google conseguiam direcionar os utilizadores para a respetiva localização. Na sua página de boas-vindas, exigia que o utilizador inserisse um nome de utilizador e uma *password* para aceder ao fórum. Nessa página de boas-vindas, um *banner* mostrava duas meninas pré-adolescentes parcialmente desnudas, com as pernas abertas, suficientemente sugestivo para o conteúdo que seria disponibilizado aos utilizadores – tradução nossa a partir do texto da decisão do caso exposto.

[10] Em termos sucintos e disponível em fonte aberta, um *script* é um conjunto de instruções ou comandos escritos para serem executados por um *software* ou sistema. Diferente dos programas tradicionais que precisam de uma estrutura mais rígida, os scripts são mais flexíveis e são usados, principalmente, para automação, integração de sistemas e geração de interatividade em *sites* e aplicativos.

informação do servidor infetado com o NIT…essa informação é complementada com as instruções do *script*. Assim, o utilizador, sem se aperceber acaba por descarregar o *script* para o seu computador onde quer que este se encontre. Uma vez descarregado e instalado o NIT executa uma sequência de instruções que recolhe as seguintes informações do computador do utilizador:

- O endereço *internet Protocol* (IP) do utilizador;
- Uma assinatura única gerada pelo NIT para que as actividades do utilizador na rede Tor possam ser identificadas;
- O sistema operativo do utilizador;
- Se o NIT já está instalado no computador do utilizador;
- O nome do sistema (*host name*[11]) utilizado para identificar o dispositivo noutros tipos de comunicação eletrónica;
- O nome de utilizador activo do sistema operativo e;
- O endereço de controlo de acesso aos meios de comunicação do utilizador, que identifica o local onde o computador do utilizador se liga à Internet.
- O NIT transmite então todos esses dados ao FBI.

Foi com base numa declaração ajuramentada do agente do FBI contendo uma descrição pormenorizada do funcionamento da rede Tor, do conteúdo do "*Playpen*" e do funcionamento da NIT que um juiz do distrito leste da Virgínia autorizou a emissão do mandado, autorizando, por 30 dias, o uso da técnica NIT relativamente aos visitantes do *site* "*Playpen*" que ali introduzissem um nome de utilizador e palavra-passe. Durante esse período, permitiu identificar milhares de computadores que acederam ao "*Playpen"*. Após identificar *Robert Mclamb* como um dos visitantes (uma semana após o inicio da utilização da técnica, o mesmo introduziu no *website* o nome de utilizador e palavra-passe, acionando o NIT), o FBI após obter um segundo mandado de busca e apreensão realizou uma busca ao seu domicílio e apreendeu-lhe o computador e dois discos rígidos, acusando-o de recebimento e posse de pornografia infantil (estariam na sua posse 2700 imagens e vídeos de pornografia infantil).

O Recorrente Robert Mclamb requereu que a recolha de prova efetuada no disco rígido não fosse considerada, com o fundamento de ter sido obtida com base num

[11] O *host name* identifica um dispositivo numa rede. É utilizado para distinguir um computador ou servidor de outros na mesma rede, facilitando a comunicação entre eles. O *host name* pode ser um nome simples, como o "meu-computador", ou pode ser parte de um domínio mais complexo, como "servidor.exemplo.com".

mandado inválido. Contestou a especificidade do mandado e sua execução, bem como a competência de jurisdição do juiz que autorizou a busca.

O Tribunal Distrital negou provimento à moção, recusa essa confirmada pelo Tribunal de recurso. Este último, fundamentou referindo que mesmo que o mandado fosse inconstitucional, o Tribunal distrital negou corretamente a moção apresentada para invalidar a recolha de prova efetuada, porque a exceção de boa-fé de *Leon*, era aplicável[12].

Nesta decisão a ajudar e suportar muito do que pretendíamos ilustrar com estes dois exemplos, surge uma referência ao facto de ao tempo da investigação do "*Playpen*", os Tribunais de 1ª Instância (*lower courts*), sob fundamento de invocação da mesma *Rule 41*, tinham entendimentos diferentes no que diz respeito ao uso de técnicas remotas (ocultas) de investigação. A título comparativo citaram os exemplos de *United States v. Laurita, No. 8:13-cv-107, 2016 WL 4179365*, que autorizou o uso de um aparelho de rastreamento e que o NIT é análogo a um aparelho desse género, com o acima referido *In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013)*, que concluiu que o mandado NIT excedeu a jurisdição do juiz.

Ao tempo, ainda nenhum Tribunal de recurso se tinha pronunciado acerca do problema.

1.3 Dados estatísticos de cibercriminalidade, necessidade de realização de pesquisas informáticas transfronteiriças e dificuldades de localização da prova digital (*loss of location*).

Não se mostra necessário apelar muito à nossa memória coletiva para nos apercebermos das vulnerabilidades de segurança informática de muitos organismos, instituições, serviços nacionais e internacionais, exploradas por grupos organizados de criminosos, que culminam em vários tipos de ataques informáticos, dificultando ou até mesmo impossibilitando o acesso aos respetivos servidores, ocasionando, inúmeras

[12] Na decisão, o Tribunal de Recurso referiu que no contexto de supressão de uma *Rule*, analisariam as questões legais novamente recorrendo ao caso *Estados Unidos v. Castellanos, 716 F.3d 828, 832 (4ª Cir. 2013)*. Nesse caso o recorrente contestou a particularidade e a execução do mandado NIT, bem como a competência jurisdicional do juiz que autorizou a emissão. Mesmo que alguma destas alegadas falhas constitua uma violação constitucional, a supressão não é uma solução adequada se a exceção de *boa fé* for aplicável nos termos de *United States v. Leon, 368 U.S. 897 (1984)*. Três Tribunais do mesmo circuito judicial analisaram o mesmo mandado NIT, que estaria em causa naquele caso. Cada um deles concluiu que, mesmo que o mandado NIT viole a Quarta Emenda, a exceção de *boa fé* de *Leon* impede a supressão das provas. Ver *Estados Unidos v. Horton, 863 F.3d 1041 (8ª Cir. 2017); Estados Unidos v. Levin, 874 F.3d 316 (1ª Cir. 2017); Estados Unidos v. Workman, 863 F.3d 1313 (10ª Cir. 2017)*. Nós concordamos. – Tradução nossa a partir da decisão exposta.

vezes, o colapso de prestação de vários tipos de serviços (*v.g.* operadores de comunicações e prestadores de cuidados de saúde).

A nível nacional, de acordo com o Relatório Anual de Segurança Interna (RASI) 2024[13], a criminalidade informática participada apresentou uma diminuição de 20 casos (-0,8%). Nas tipologias de crimes que integram a categoria, temos o acesso indevido ou ilegítimo, interceção ilegítima (+3,9%), falsidade informática (-7,9%), sabotagem informática (-21,3%, outros crimes informáticos (+79,7%), viciação ou destruição de dados, dano relativo a dados programas (+22,7%), reprodução ilegítima de programa protegido (+450%).

No primeiro relatório da Europol acerca das redes criminosas mais perigosas a operar no espaço europeu, apurou-se a existência de 821 redes criminosas, com 25000 membros com capacidade de praticar crimes em simultâneo em vários países, impactando com essa atividade nociva na segurança e vida de milhões de cidadãos europeus[14].

Relativamente aos crimes praticados, apesar da existência de realidades dispersas metade das redes identificadas dedica a sua atividade ou está envolvida em negócios relacionados com o tráfico de estupefacientes. A segunda atividade mais comum destas redes está relacionada com esquemas fraudulentos, sendo que, das 821 redes identificadas, 50 estão especializadas em atrair vítimas para vários tipos de fraudes *online*, principalmente em áreas de investimentos ou esquemas românticos[15].

Ainda de acordo com o relatório, foram identificadas 9 redes criminosas, cuja atividade principal e especialidade está relacionada com ciberataques. O envolvimento de outras redes nesta área surge, como suporte às atividades de fraude e lavagem de dinheiro a que se dedicam. Estas redes estabelecem operações num modelo de negócio filiado, no âmbito do qual uma (a principal) cria e disponibiliza, mediante um pagamento, o *malware* aos afiliados (*ransomware-as-a-service*) para que estes realizem operações de *ransomware* (ataques cibernéticos), negociando depois e exigindo o pagamento de avultadas quantias em ativos digitais (criptomoedas) às vítimas, que depois repartem entre si.

---

[13] Fonte disponível na internet: <URL:https://www.portugal.gov.pt/pt/gc24/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-rasi-2024>. [Consultado em 06/04/2025].

[14] Europol (2024), *Decoding the EU´s most threatening criminal networks*, *Publications Office of the European Union, Luxembourg.* Disponível na internet:<URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf>. [Consultado em 03/07/2024].

[15] *Ibidem*, cit., p.30.

Foi com o esforço das autoridades judiciárias e forças policiais, que no ano de 2024, foram noticiadas intervenções policiais da Europol contra este tipo de criminalidade, a primeira contra os servidores do *Genesis Market*, controlados por uma rede que dedicava a sua atividade a vender credenciais de acesso roubadas às vítimas, a *hackers* de todo mundo. Este "mercado" vendia as chamadas *bots*[16] que infetavam dispositivos das vítimas através de *malware* ou ataques de controlo de conta de utilizador. Estas *bots* permitiam o acesso por parte destes criminosos aos dispositivos das vítimas e a todos os dados ali armazenados, tais como *logins* e *passwords*. Os preços de venda, por *bot*, variavam de acordo com o número e natureza dos dados ilicitamente obtidos e poderiam situar-se entre USD 0.70 e várias centenas de dólares. As mais dispendiosas, seriam as que continham informação financeira, que permitiam o acesso a contas bancárias *online*[17].

A segunda, uma ação coletiva de autoridades policiais de 10 países contra uma rede internacional criminosa, o grupo de *ransomware LockBit*, comprometendo a atividade da sua principal plataforma e outras infraestruturas da atividade criminosa, nomeadamente, 34 servidores nos Países Baixos, Alemanha, Finlândia, França, Suíça, Austrália, Estados Unidos e Reino Unido. A pedido de autoridades judiciárias francesas, foram ainda detidos 2 indivíduos, na Polónia e Ucrânia. As autoridades apreenderam ainda mais de 200 contas de ativos digitais (criptomoedas) pertencentes à organização[18].

Vemos, pois, como a atividade destas organizações criminosas, explorando os mais jovens e outros estratos da sociedade mais vulneráveis (como os idosos que por vezes perdem as poupanças de uma vida), afeta não só os cidadãos europeus, mas de todos aqueles que sejam as suas vítimas em qualquer parte do mundo.

Temos bem presente a grande capacidade de meios e recursos que estas organizações criminosas dispõem, a facilidade com que recorrem a indivíduos com conhecimentos especializados em várias áreas (*v.g.* advogados, contabilistas, químicos, informáticos, motoristas) para dissimular, ocultar áreas de atuação e proveitos através de técnicas antiforenses (que visam dificultar a localização e identificação dos criminosos) frustrando e inviabilizando que as autoridades judiciárias, muitas vezes nem sequer se apercebam da conjugação de esforços que mantém entre si.

---

[16] Programa autónomo na internet ou noutra rede apto a interagir com outros sistemas ou utilizadores.

[17] Europol, 5 April, *Takedown of notorious hacker marketplace selling your identity to criminals*, disponível na internet:<URL:https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals>. [Consultado em 03/07/2024].

[18] Europol, 20 February 2024, *Law enforcement disrupt world's biggest ransomware operation*, disponível na internet:<URL:https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>. [Consultado em 03/07/2024].

Tendo presente esta realidade, pensemos agora, num qualquer tipo de crime grave (homicídio, tráfico de estupefacientes, abuso sexual de menores), no âmbito do qual o Ministério Público (MP) no despacho de promoção de realização das buscas, promova, nos termos constantes do artigo 15.º, n.º 1 da Lei n.º 109/2009, de 15 de setembro (LCc), a pesquisa e apreensão de elementos de prova que possam estar armazenados em sistemas informáticos que se encontrem no local visado. E no local, a prova digital pode estar em todo o lado: em servidores, nas redes e sistemas informáticos, na internet, em redes sociais, em sistemas de mensagens instantâneas, em redes *peer-to-peer* (P2P), em arquivos de imagem e vídeo e respetivos metadados, em *smartphones* e dispositivos a eles conectados por *Wireless* ou *Bluetooth*, dispositivos de armazenamento, como sejam discos rígidos ou unidades de USB, apenas para citar alguns a título de exemplo.

Também aqui, no decurso da realização destas pesquisas informáticas, pode ocorrer não só que a informação (dados informáticos) possa estar armazenada em sistemas de computação em nuvem (*clouds)* de países com fornecedores de serviço perfeitamente identificáveis (ou não) e relativamente aos quais, facilmente possam ser desencadeados mecanismos de cooperação judiciária internacionais, como por vezes, a informação pesquisada encontrar-se na *dark web*, como vimos, sem que se mostre possível identificar de forma cabal o país ou países, caso esta esteja replicada ou fragmentada, onde a mesma possa estar armazenada.

Na realidade, com a cada vez maior disseminação da informação, existência de serviços de computação em nuvem que levam a que os dados informáticos estejam armazenados remotamente (na *cloud*) ao contrário do tradicional armazenamento em equipamento(s) em posse do utilizador, técnicas de ocultação[19] utilizadas por particulares e redes criminosas, são cada vez maiores os obstáculos com que os investigadores se deparam no âmbito das investigações que tem a cargo. Se a acrescer a tudo quanto ficou exposto, juntarmos a volatilidade que consubstancia este tipo de prova, facilmente camuflável ou mesmo eliminável, apercebemo-nos que estas pesquisas e recolhas de prova, enfrentam verdadeiros obstáculos jurídicos, por vezes, inultrapassáveis por questões relacionadas com a soberania dos Estados. Na verdade, em inúmeras investigações, os OPC são confrontados com dificuldades e por vezes «…impossibilidade de estabelecer com razoabilidade a localização física do agente, da infraestrutura

[19] Já aqui abordamos o acesso através de *browsers* como o Tor. A título meramente informativo podemos acrescentar os exemplos dados em (ANTUNES, 2023, p.577), como sejam o *Freenet* ou o *I2P*, os *Proxys* e os serviços de *Virtual Private Network* (VPN).

criminosa ou da própria prova digital. A esta adversidade dá-se o nome de *loss of location*»[20].

Nas conclusões do Conselho sobre a melhoria da justiça penal no Ciberespaço, de 9 de junho de 2016, o Conselho da União Europeia, referindo-se a esta realidade, comprometeu-se a «…explorar a possibilidade de uma abordagem Europeia comum no âmbito da jurisdição no Ciberespaço, […], perante situações em que um número elevado de sistemas de informação sejam utilizados em simultâneo em várias jurisdições para o cometimento de apenas um crime, situações em que a prova digital se movimente, em períodos temporais curtos, por várias jurisdições ou que sejam utilizados meios sofisticados para ocultar a localização da prova digital ou atividade criminosa, daqui resultando *loss of location*»[21].

Veremos como os esforços de tornar mais céleres e ágeis os mecanismos de cooperação judiciária, ainda assim se revelam ineficazes quando estamos perante necessidades de recolha expedita deste tipo de provas digitais, conceito esse que tentaremos elucidar de seguida.

1.4 Conceito e relevância, da distinção entre ambiente digital, prova eletrónica e prova digital

No âmbito das diligências de investigação no ciberespaço (mas também de outro tipo de criminalidade), a prova apresenta-se como elemento primordial, senão central, dessas investigações. É a prova que habilita firmar ou infirmar factos imputados e vertidos num despacho de acusação e é ela que permite, fundamentar e suportar uma eventual condenação em sede de audiência de discussão e julgamento.

A rápida e constante evolução tecnológica tem vindo a dificultar esta tarefa, algo a que o legislador nacional não ficou imune. «O legislador português, não tendo – compreensivelmente - esboçado qualquer definição de prova digital na teia legislativa aplicável, acabou por criar espaço para que a jurisprudência e a doutrina preenchessem o vazio deixado com a formulação de termos conceptualmente sobreponíveis. Em particular, a alternância pouco clara entre os conceitos de prova «*guardad[a] em suporte*

[20] (ANTUNES, 2023, p. 572).
[21] Tradução nossa a partir do original cf. *Council conclusions on improving criminal justice in cyberspace*, p.5, ponto 10, disponível na internet:<URL:https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf#page=5>. [Consultado em 19/06/2024].

digital» e de «*prova em suporte electrónico*» criaram, a nosso ver incorrectamente, a ideia de sinonímia entre os conceitos de prova electrónica e prova digital»[22].

O legislador nacional, não consagrou desde logo a autonomia da prova digital em regulamentação legal autónoma, no entanto, por força de compromissos internacionais assumidos, a reforma do Código de Processo Penal (CPP) de 2007, através da Lei n.º 48/2007, de 29 de agosto, viria, através de uma nova redação, a colocar o artigo 189.º do CPP como disposição central a esse respeito. Em simultâneo, nesse ano e nos que se seguiram, para além deste diploma legal, introduziram-se ainda dois novos diplomas no ordenamento jurídico português, a Lei n.º 32/2008, de 17 de julho, que transpôs para a nossa ordem jurídica a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, aplicável aos *"crimes graves"* e, principalmente, a Lei n.º 109/2009, de 15 de setembro (a Lei do Cibercrime) que adiante melhor abordaremos neste trabalho, complementando a regulação para efeitos de obtenção de prova digital.

Esta dispersão legislativa de regulação da prova digital, com definições e emprego de terminologia técnica pouco precisa, acabou por gerar e criar dificuldades práticas no âmbito da sua aplicação, motivo pelo qual assumimos a importância de estabelecer, com clareza, uma definição conceptual do que seja a prova digital. Aliás, atenta a proliferação de casos que tem como base a recolha de elementos de prova carreados para o processo de natureza digital, poder-se-ia equacionar uma revisão do CPP no Título II (Dos meios de prova) e, para além da prova testemunhal, da prova por acareação, da prova por reconhecimento, da prova pericial e da prova documental, incluir-se um novo capítulo "Da prova digital".

Assim, para além do uso dos termos de prova eletrónica e prova digital, por vezes verificamos também referência a ambiente digital, que pese embora seja desprovido de significado jurídico, importa ainda assim ter presente. Na formulação de DAVID SILVA RAMALHO, que importamos para este estudo, «[a noção] afigura-se útil e operativa como meio para assinalar, de forma facilmente compreensível, a distinção entre o contexto físico, materializado numa envolvência sensorialmente apreensível, e o contexto digital, impercetível aos sentidos sem a mediação de sinais eléctricos e gerador de um *espaço*

[22] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017. ISBN 978-972-40-7000-1. p. 99.

distinto mas inegavelmente desprovido de materialidade. Tal como entendemos, o conceito de ambiente digital engloba apenas os dados informáticos que, de algum modo, são criados, processados, armazenados e são identificáveis em sistemas informáticos, de modo a que podem ser acedidos direta ou remotamente. Será, portanto, aquilo que jaz em forma binária e que é virtualmente acessível a um utilizador através da mediação de tecnologias de informação. Daqui decorrem duas noções distintas: o ambiente digital geral e o ambiente digital pessoal.

O primeiro representa, em síntese, todo o *espaço* digital no qual existem dados informáticos acessíveis, direta ou remotamente, por utilizadores de tecnologias de informação, no qual existe uma aparência de envolvência virtual suscetível de permitir aos seus utilizadores tratar e interagir com informação. Poderá incluir-se aqui o acesso à Internet, a uma Intranet, ou mesmo, em abstrato, a suportes de armazenamento.

Já a noção de ambiente digital pessoal incluirá, na formulação de GONZÁLEZ-CUELLAR SERRANO, que poderemos importar para o presente estudo, um contexto «composto pela informação em forma electrónica, magnética ou luminosa que, voluntária ou involuntariamente, de forma consciente ou inconsciente, [o utilizador] gera com a sua actividade, independentemente de onde se encontrem os arquivos informáticos que a contenham ou os canais de comunicação através dos quais discorra. Seja durante um instante, seja transitória ou permanentemente, uma boa parte dos actos da pessoa deixam um rasto energético, em algum meio ou lugar, susceptível de servir como fonte de conhecimento da realidade»[23].

Tendo presente o conceito de ambiente digital e o que nos propusemos analisar no âmbito deste estudo, como bem se percebe, a prova digital poderá *viajar* e *estar presente* em simultâneo nestes dois *espaços* digitais. Devemos perceber que a informação guardada num sistema informático, tanto pode assumir a forma estática (*v.g.* no disco rígido do próprio computador ou sistema de armazenamento físico local) como também dinâmica, se pensarmos naquela que é guardada em sistemas de computação em nuvem, com o constante envio e reenvio de informação entre os seus diversos servidores, como já tivemos oportunidade de verificar.

Na verdade, a informação presente no ambiente digital (geral ou pessoal) é diferente daquela que *circula* em rede, motivo pelo qual deverá existir um cuidado acrescido na análise dos dados de comunicação em trânsito (os dados de tráfego e de localização

[23] *Apud* (RAMALHO, 2017, pp. 37-38).

relativos a pessoas singulares e coletivas, bem como os dados de identificação do assinante ou de utilizador registado junto do prestador de serviços) que se encontram presentes e são objeto de regulação no regime de interceções de comunicações, que não abordaremos neste trabalho.

Percebemos as dificuldades do legislador nacional e a dispersão legislativa de regulação da prova digital, que em muito decorre das inúmeras definições que constam de *guidelines*, diplomas internacionais e nacionais relevantes nesta matéria, sendo percetível o porquê da distinção pouco clara que tem surgido entre estes dois conceitos (prova digital e prova eletrónica). Elencaremos algumas das definições que ali constam, por vezes relacionadas com questões que envolvem a recolha e tratamento da prova digital, importantes para a integridade, fiabilidade e validade da mesma em sede de audiência de discussão e julgamento.

1.5 Definições prova digital que constam de *guidelines*, diplomas internacionais e nacionais.

Assim, de acordo com definições do ***International Principles for Computer Evidence***[24], apresentadas pelo *Scientific Working Group on Digital Evidence* (SWGDE)[25] no que foi o trabalho para o desenvolvimento de diretrizes e padrões interdisciplinares para a recuperação, preservação e exame de evidências digitais, incluindo áudio, imagem e dispositivos eletrónicos **a prova digital** surge definida como "*informação guardada ou transmitida em formato digital com valor probatório em tribunal*".

No ***ISO***[26]***/IEC 27037:2012****(en) Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital*

[24] Tradução nossa a partir do original disponível na internet:<URL:https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Definitions>. [Consultada em 21/04/2025].

[25] A *International Organization on Computer Evidence* (IOCE), criada em 1995, desenvolveu esforços no sentido de providenciar às agências internacionais e autoridades judiciárias um fórum para troca de informações relativas à investigação de crimes informáticos e questões forenses relacionadas. Em resposta ao Comunicado e aos planos de acção do G-8 de 1997, a IOCE foi incumbida do desenvolvimento de normas internacionais para o intercâmbio e recuperação de provas electrónicas. Em 1998 surgiu o *Scientific Working Group on Digital Evidence* (SWGDE).

[26] A ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*) formam o sistema especializado para uniformização/padronização mundial em questões relacionadas com informação/actividade tecnológica. As normas internacionais emanadas e esta em particular, que se refere a dados que já estão em formato digital, fornecem diretrizes e procedimentos a seguir no tratamento de potenciais provas digitais. Os procedimentos referem-se à identificação, recolha, aquisição e preservação de provas digitais e visam assegurar aos investigadores/especialistas envolvido uma metodologia na obtenção destas provas que contribuam para a manutenção da autenticidade e integridade por forma a sustentar de forma credível a sua fiabilidade e aceitação como prova em Juízo. Tradução nossa a partir do original disponível na internet:

evidence[27], a **prova digital** surge como "*Informação ou dados, armazenados ou transmitidos em formato binário com valor probatório em tribunal*". É nesta norma que também se faz referência ao responsável inicial pela recolha de prova digital - *Digital Evidence First Responder* (DEFR), em Inglês – indivíduo autorizado, treinado e devidamente qualificado para, num cenário de incidente que envolva aquisição e recolha de provas digitais, atuar com responsabilidade no manuseamento dessas provas, bem como ao Especialista em prova digital - *Digital Evidence Specialist* (DES), em Inglês – individuo apto e habilitado a desempenhar funções de responsável inicial pela prova digital (*DEFR),* com conhecimentos especializados, habilitações e capacidades que lhe permitam lidar com um largo espectro de problemas técnicos (nota: um DES pode ter habilidades adicionais específicas, por exemplo, aquisição de rede, aquisição de RAM, conhecimento de software de sistema operacional ou conhecimento de *mainframes*. Nesta norma faz-se ainda referência aos sistemas de armazenamento digital, locais de preservação das provas digitais (relacionado com a segurança e condições onde as provas digitais são armazenadas), preservação da integridade ou condição original dessa prova, bem como, modo de recolha das provas que deve ser o menos intrusivo possível, com recurso, tanto quanto possível, a *backups*.

Ainda no plano terminológico e para os fins presentes na **Convenção sobre o Cibercrime**[28] (CBCc) consta com interesse e relevo a definição de **sistema informático** "*equipamento ou conjunto de equipamentos interligados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o tratamento automatizado de dados*" e **dados informáticos** como sendo "*qualquer representação de factos, informações ou conceitos numa forma adequada para o processamento informático, incluindo um programa que permita a um sistema informático executar uma função*".

Na **Decisão-Quadro 2005/222/JAI**[29] relativa a ataques contra os sistemas de informação, encontramos a definição de **sistema de informação** "*qualquer dispositivo*

<URL:https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27037:ed-1:v1:en>. [Consultado em 21/04/2025].

[27] Tradução nossa a partir do original disponível na internet: <URL:https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27037:ed-1:v1:en>. [Consultada em 21/04/2025].

[28] Convenção do Conselho da Europa sobre o Cibercrime, assinada pelos Estados Membros e outros Estados em Budapeste, 23.XI.2001, disponível na internet:<URL:https://rm.coe.int/1680081561>. [Consultado em 21/04/2025]. Tradução nossa.

[29] Decisão-Quadro 2005/222/JAI do Conselho de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, entretanto substituída pela Diretiva 2013/40/EU do Parlamento Europeu e Conselho, de 12 de agosto de 2013, disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32005F0222>. [Consultado em 21/04/2025].

ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, protecção e manutenção" e **dados informáticos** como "*qualquer representação de factos, informações ou conceitos, de forma a serem processados num sistema de informação, nomeadamente um programa capaz de permitir que um sistema de informação execute uma dada função*".

Até ao momento da entrada em vigor da **Lei do Cibercrime** (LCc)[30] o ordenamento jurídico português era omisso relativamente a regras especiais relativas à recolha de prova em suporte eletrónico, socorrendo-se, no âmbito da investigação da criminalidade relacionada com meios informáticos, dos mecanismos e regras gerais do Código de Processo Penal. Transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa, anteriormente referidas, a LCc procurou, assim, condensar num só diploma legislativo todas as normas respeitantes à criminalidade informática: normas de direito substantivo, normas de direito processual e normas relativas à cooperação judiciária internacional. Aqui encontramos, com relevo e entre outros, a definição de **sistema informático** "*qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção*" e **dados informáticos** "*qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função*".

Por sua vez, consta da **Diretiva 2013/40/EU** do Parlamento Europeu e do Conselho[31], definições de **Sistema de informação** "*um dispositivo ou grupo de dispositivos*

[30] Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), disponível na internet: <URL:https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis>. [Consultado em 21/04/2025].

[31] Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, disponível na internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040#page=5>. [Consultado em 21/04/2025].

interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção" e **dados informáticos** "*uma representação de factos, informações ou conceitos de forma adequada para o tratamento num sistema de informação, incluindo um programa que permite que um sistema de informação execute uma dada função*".

Por fim as definições, que constam do **Regulamento e Diretiva e-Evidence**. Cinco anos após o início das negociações, o Conselho e o Parlamento Europeu (PE), finalmente, adotaram os atos legislativos conducentes à implementação de um novo sistema de recolha de provas eletrónicas em processos criminais na União Europeia (UE).

A legislação, publicada no Jornal Oficial (JO) da UE no dia 28 de julho de 2023, teve como objetivo disponibilizar aos Estados Membros, alternativas – mais rápidas e eficientes – às ferramentas de cooperação internacional e assistência jurídica mútua atualmente existentes, abordando e focando essencialmente nos problemas que decorrem da natureza volátil das provas eletrónicas e também de questões relacionadas com a "perda de localização" dos dados armazenados.

As novas regras sobre provas eletrónicas consistem em duas medidas legislativas: O **Regulamento (UE) 2023/1543** do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais[32]. Neste diploma, dispõem-se as regras de acordo com as quais uma autoridade de um Estado-Membro, no âmbito do processo penal, poderá proceder à emissão de uma Ordem Europeia de Entrega de Provas ou uma Ordem Europeia de Conservação de Provas e, assim, ordenar (diretamente) a um prestador de serviços que disponibilize a oferta de serviços na União (quer esteja estabelecido ou com representação legal noutro Estado-Membro, que produza ou conserve provas eletrónicas, independentemente da localização dos dados. Consta para efeitos do regulamento, as seguintes definições: **Prova eletrónica** "*dados de assinantes, dados de tráfego ou dados de conteúdo, conservados em formato eletrónico, por um prestador de serviços ou em seu nome, no momento da receção de um certificado de*

[32] Publicado JOUE L 191 de 28/07/2023, pp.118-180, disponível na internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2023:191:FULL#page=120>. [Consultado em 21/04/2025].

ordem europeia de produção (COEP) ou de um certificado de ordem europeia de conservação (COEC)", **Dados solicitados com o único objetivo de identificar o utilizador** "*os endereços IP e, se necessário, as portas de origem e o carimbo temporal pertinentes, nomeadamente a data e a hora, ou os equivalentes técnicos desses identificadores e informações conexas, quando solicitados pelas autoridades responsáveis pela aplicação da lei ou pelas autoridades judiciais com o único objetivo de identificar o utilizador numa investigação criminal específica*", **dados de tráfego** "*dados relacionados com a prestação de um serviço por um prestador de serviços que servem para fornecer contexto ou informações adicionais sobre esse serviço e que são gerados ou tratados por um sistema de informação do prestador de serviços, tais como o remetente e o destinatário de uma mensagem ou de outro tipo de interação, sobre a localização do dispositivo, a data, a hora, a duração, o tamanho, a via, o formato, o protocolo utilizado e o tipo de compressão, e outros metadados das comunicações eletrónicas e dados, com exceção dos dados de assinantes, relacionados com o início e o fim da sessão de acesso de um utilizador a um serviço, tais como a data e a hora da utilização, o início («log-in») e o fim («log-off») da ligação ao serviço*", **dados de conteúdo** "*dados num formato digital, como texto, voz, vídeos, imagens e som, que não sejam dados de assinantes ou de tráfego*", **sistema de informação** "*um sistema de informação na aceção do artigo 2.º, alínea a), da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho*", para além de outros como sejam a definição de **prestador de serviços** "*qualquer pessoa singular ou coletiva que presta uma ou mais das seguintes categorias de serviços, com exceção dos serviços financeiros a que se refere o artigo 2.º, n.º 2, alínea b), da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho*[33]*"* aludindo aos serviços de comunicações eletrónicas na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2018/1972[34] e outros serviços da sociedade da informação a que se refere o artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535[35].

[33] Diretiva 2006/123/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa aos serviços no mercado interno, disponível na internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0123#page=16>. [Consultado em 21/04/2025].

[34] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho de 11 de dezembro de 2018 que estabelece o Código Europeu das Comunicações Eletrónicas, disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L1972#page=64>. [Consultado em 21/04/2025].

[35] Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (codificação), disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L1535#page=3>. [Consultado em 21/04/2025].

Por sua vez, a **Diretiva (UE) 2023/1544** do Parlamento Europeu e do Conselho, de 12 de julho de 2023, que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais[36].

Encontram-se aqui estabelecidos, para os prestadores de serviços que oferecem serviços na União, as regras relativas à designação de estabelecimentos designados e à nomeação de representantes legais, bem como os procedimentos para efeitos de recolha de provas eletrónicas em processos penais, nomeadamente, para receção, cumprimento e execução de decisões e ordens emitidas pelas autoridades competentes dos Estados-Membros.

Para efeitos de diretiva e com relevo, consta a definição de "**prestador de serviços**" nos exatos termos que consta do supra referido Regulamento (UE) 2023/1543.

1.6 Prova eletrónica e prova digital.

Este percurso de análise das definições acima expostas, sem nos arvorarmos defensores do legislador nacional, teve como propósito percebermos se, efetivamente, o espaço que este deixou, ao não deixar devidamente clarificado e expresso o conceito de prova eletrónica e prova digital nomeadamente, quando se refere no artigo n.º 189.º do CPP ao conceito de prova «guardadas em suporte digital» e nos artigos 1.º, 11.º, n.º 1, alínea c), 18.º, n.º 1, alínea b) e 20.º da LCc quando refere «prova em suporte electrónico», potenciou de facto, como defende alguma doutrina e jurisprudência, a ideia que uma e outra se referem à mesma realidade.

Poderemos estar, eventualmente, tentados a considerar esta distinção despicienda e os juristas menos letrados tecnologicamente, porventura, concordarem com a visão da suficiência de compreensão da prova digital e da sua recolha em termos superficiais. A complexidade técnica que a prova digital assume, não justifica que a nível do seu enquadramento dogmático e legislativo, esta seja muitas vezes sujeita a uma recorrente analogia conceptual com os demais meios de prova.

Na verdade, como já vimos, são inúmeros os dispositivos aptos a criar e armazenar dados em formato digital que posteriormente poderão ser utilizados como prova, motivo

[36] Publicado JOUE L 191 de 28/07/2023, pp.181-190, disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2023:191:FULL#page=183>. [Consultado em 21/04/2025].

pelo qual releva a distinção entre a prova digital e a prova proveniente de dispositivos analógicos.

Na ausência de uma formulação distintiva entre prova eletrónica e prova digital operada pelo legislador nacional, vejamos, ainda que de forma breve, como esta vem sendo abordada.

A nível doutrinário, PAULO DÁ MESQUITA refere-se a ambos da seguinte forma «[a] temática da prova electrónica que, a traço grosso, compreende a prova que se apresenta na forma digital e não em suporte de papel ou outro meio tangível[…]»[37] e DAVID SILVA RAMALHO trazendo ensinamentos de GEORGE R.S. WEIR E STEPHEN MASON, quando estes referem que «o termo prova electrónica é amplamente utilizado, mas é comummente utilizado para indicar prova digital, o que acrescenta confusão. Sugere-se que o termo prova electrónica é um termo generativo, em vez de um termo específico, na medida em que engloba todas as formas de dados, quer sejam produzidos por um dispositivo analógico, ou em forma digital. As duas formas de prova não devem ser confundidas, porque diferentes procedimentos probatórios e processuais se aplicam a cada forma de prova». Os referidos autores acabam por oferecer uma definição de prova electrónica que se traduz em «dados (compreendendo o resultado de dispositivos analógicos ou dados em formato digital) que são manipulados, armazenados ou comunicados através de qualquer dispositivo, computador ou sistema informático feito pelo Homem, ou transmitidos através de um sistema de comunicação que têm o potencial de tornar a explicação factual de qualquer parte mais provável ou menos provável do que seria sem a prova»[38].

Revela-se, determinante, para os autores, perceber o resultado que advém do dispositivo, na medida em que estes consideram a prova electrónica abrangente, nela incluindo os dados em formato digital, mas também aqueles que se encontram em formato analógico (*v.g.* gravações em fita de vídeo e áudio ou fotografias de rolo fotográfico). Será, pois, o resultado a determinar se estamos perante prova analógica ou prova digital, concluindo DAVID SILVA RAMALHO a respeito do entendimento destes autores que «Deste modo, a definição de prova digital será encontrada, na medida da sua adaptação à definição de prova electrónica, excluindo toda a prova analógica, e vice-versa»[39],

[37] MESQUITA, Paulo Dá, *Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal português – o Código e a Lei do Cibercrime* in *Processo Penal, Prova e Sistema Judiciário*, 1ª Edição. Coimbra: Coimbra Editora, 2010, ISBN 978-972-32-1842-8. p. 84.
[38] (RAMALHO, 2017, pp. 99-100).
[39] *Ibidem*, cit. p. 100.

realçando e destacando a importância de sabermos de facto do que se trata e no que consiste a prova digital.

Esta noção de uma maior amplitude da prova electrónica em relação à prova digital, com o uso daquela em substituição desta, acabou por sair reforçada no parágrafo 141 do Relatório Explicativo da Convenção sobre o Cibercrime, nos termos da qual a *«prova electrónica»* referida no artigo 14.º, n.º 2, alínea a) da Convenção, abrange «[…] a informação contida em formato digital ou outro formato electrónico poder ser utilizada como prova, no contexto de acções penais em Tribunal, independentemente da natureza da infracção penal que está a ser julgada»[40].

Não será por isso estranho, verificar por parte de alguma doutrina mais formal, o uso da expressão mais genérica de prova electrónica em substituição do termo prova digital, e também já nos apercebemos, pelas razões expostas, que esta talvez não se revele a melhor opção, por utilizar conceitos distintos como sinónimos.

Por outro lado, também é comum vermos por vezes o uso da expressão *electrónico-digital* conforme BENJAMIM RODRIGUES, que a ela se refere como «*qualquer tipo de informação, com valor probatório, armazenada* [em repositório electrónico-digitais de armazenamento] *ou transmitida* [em sistemas e redes informáticas ou rede de comunicações electrónicas, privadas ou publicamente acessíveis], *sob a forma binária ou digital»*[41], sem que antes, este mesmo autor, em momento prévio na mesma obra, confesse que se sentiu tentado a definir prova digital, 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"*[42].

O uso de expressão electrónico-digital, principalmente, se utilizado como sinónimo de prova digital e tendo como objectivo realçar que se trata de uma subespécie de prova electrónica, como parece ter sido esse o propósito do autor, poderia parecer acertado, no entanto, é o próprio que transparece a possibilidade de poder não ter sido essa a sua intenção, ao referir «A investigação criminal "em ambiente electrónico-digital", impõe

---

[40] Relatório Explicativo da Convenção sobre o Cibercrime, disponível na internet: <https://rm.coe.int/16802fa429#page=29>. [Consultado em 21/04/2025].

[41] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV – Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital*, Coimbra, 2011, p. 39. Do mesmo autor, *Direito Penal – Parte Especial – Tomo I – Direito Penal Informático-Digital*, Coimbra, 2009, p.722.

[42] (RODRIGUES, 2011, p.30) e de igual forma (RODRIGUES, 2009, pp. 510-511).

novas exigências ao processo penal português, já que se afigura imprescindível tomar em linha de conta as específicas características da chamada prova ["*electrónico*"] digital" ("*electronic evidence*" ou "*digital evidence*")»[43].

Constatamos, desta forma, que o termo *digital* pode estar presente em vários dispositivos e sistemas tecnológicos de comunicação não electrónicos, no entanto, incontornavelmente, encontra-se associado à lógica binária (representação matemática da informação que utiliza apenas dois valores: verdadeiro (representado pelo 1) e falso (representado pelo 0). Cada um destes dígitos representa um *bit*, a unidade mais pequena processada por dispositivos digitais e, de uma forma mais abrangente, à informática se relacionado com a palavra prova, razão pela qual a alusão a prova electrónico-digital nos parece mais acertada, principalmente, se tiver como propósito ressalvar que se trata de uma subespécie da prova electrónica.

Já nos apercebemos da presença da prova digital num grande universo de equipamentos e agora, talvez se mostre mais percetível constatar, que cada uma daquelas fontes pode conter várias categorias de prova, cada uma com diferentes especificidades relativamente aos meios de recolha (*v.g.* a recolha que é feita relativamente ao e-mail é seguramente diferente entre a que decorre num computador fixo e aquela que ocorre num *smartphone* no qual se pretenda, por exemplo, obter o registo de chamadas recebidas/efetuadas. Neste último caso, por vezes, aconselha-se, que a recolha seja efetuada com o aparelho desligado ou num ambiente isolado por forma a não causar alterações indesejadas resultantes, por exemplo, de ligações a *wi-fi hotspots* ou antenas de operadores de serviços, que possam adulterar esse registo.

Neste sentido, partilhamos do entendimento daqueles que consideram ser as especificidades próprias da prova digital, que em nada se confundem com a prova física, que justificaria um enquadramento jurídico diferente, sem necessidade de recurso a subsidiariedade de regimes pensados, sobretudo, para esta última. Justifica-se e recomenda-se um regime autónomo, com conceitos de prova eletrónica e prova digital perfeitamente clarificados e não a sua relegação para o domínio da analogia com meios de obtenção de prova (buscas e apreensões) dotadas de outras características distintivas, mais facilmente apreensíveis e que não são, de todo, de cariz eminentemente técnico, como acontece com a prova digital.

[43] (RODRIGUES, 2009, p.509).

1.7 Importância da prova digital e da sua recolha de acordo com os trâmites da ciência forense digital

Aflorámos no âmbito das definições elencadas que constam de *guidelines*, diplomas internacionais e nacionais (neste momento se revela o propósito), a importância relacionada com as especificidades da recolha da prova digital de forma segura, por forma a garantir o seu valor probatório e a distinção que deve ocorrer com outros tipos de prova.

A respeito da distinção e a título ilustrativo, DAVID RAMALHO destaca uma característica específica da prova digital, a imaterialidade ou invisibilidade, referindo «…se abrirmos fisicamente um computador, não encontraremos no seu interior documentos escritos, sons ou filmes sensorialmente apreensíveis. Há que recordar que a ilusão de tridimensionalidade que encontramos nos ecrãs dos sistemas informáticos é o produto de um processo de leitura de dados de origem eléctrica e meramente virtual e que, sem meios técnicos que permitam aceder, recolher, ou interceptar a prova digital, esta não é fisicamente apreensível»[44].

É por este motivo que existem cuidados redobrados na recolha dos vestígios de crime presentes em diferentes cenários (*v.g.* nos homicídios e roubos a agências bancárias, a recolha de vestígios de ADN ou lofoscópicos) realizados por elementos especializados dos vários OPC que são responsáveis por essas recolhas. Esses procedimentos visam salvaguardar os locais, a recolha segura dos vestígios, a preservação e integridade da prova recolhida, com vista a servirem como elementos de prova no âmbito de um processo judicial.

Por maioria de razão, deverão ser adotados procedimentos idênticos nos cenários em que nos deparemos perante recolha de prova digital, não só devido a toda a complexidade técnica associada, mas também porque o objetivo, é a preservação da sua integridade, para posterior segura e efetiva demonstração dos factos a comprovar.

2. A JURISDIÇÃO COMPETENTE EM INVESTIGAÇÕES DIGITAIS TRANSFRONTEIRIÇAS

Estabelecidos estes conceitos iniciais, relevantes na nossa perspectiva, abordaremos de seguida a questão relacionada com a jurisdição competente perante investigações que envolvam a recolha de prova digital alocada em países terceiros, eventualmente potenciadora de conflitos de jurisdição internacionais.

[44] (RAMALHO, 2017, pp. 104-105).

2.1 Conceito de soberania, território e jurisdição dos Estados.

No plano da soberania e respeito pelas fronteiras internacionalmente reconhecidas, infelizmente, a guerra na Ucrânia, retoma e recoloca o foco neste tema de grande importância do direito internacional e, futuramente, veremos se este estará à altura de tão grande desafio imposto pelo Estado agressor (Rússia), recorde-se, um dos membros permanentes do Conselho de Segurança da Organização das Nações Unidas (ONU).

Todavia, as questões de soberania e proteção dos direitos dos cidadãos nacionais que abordaremos neste estudo assumem importância e relevam, principalmente, no âmbito da criminalidade informática transnacional, motivo pelo qual consideramos importante, recordar conceitos de soberania, território e jurisdição.

O artigo 1.º da Constituição da República Portuguesa refere que "*Portugal é uma República soberana…*"[45].

O direito soberano dos Estados traduz-se no exercício exclusivo de autoridade sobre o espaço delimitado por um território, nos limites dos quais se encontra um povo. A origem etimológica do termo «território» denota já essa relação de exclusividade com um Estado. Neste sentido referimos: «Aliás, GROTIUS, em busca da origem etimológica do vocábulo "*território*", associa-lo à ação de "*aterrorizar*", na medida em que aquele que exerce autoridade dentro de tal espaço físico dispõe da capacidade de afugentar os respetivos inimigos ("*terrendis hostibulus*").

Assim sendo, conforme demonstra HAURIOU, "*na História da Humanidade, a fixação das populações ao solo foi um acontecimento imenso que permitiu, indiretamente, a formação das nações e, de seguida, dos Estados*"»[46].

A Constituição da República Portuguesa (CRP), no artigo 5.º, n.º 3, acaba por traduzir esta noção do exercício de soberania no território e de não alienação desses direitos relativamente a qualquer parte do mesmo, sem prejuízo da retificação de fronteiras. Nas relações internacionais, o artigo 7.º, n.º 1 da CRP rege que o Estado rege-se por princípios independência nacional, de respeito pela soberania e de não ingerência nos assuntos de outros Estados. Destes preceitos Constitucionais retira-se duas dimensões relativamente à soberania dos Estados: Uma dimensão interna, que fundamenta o conceito de

[45] CANOTILHO, José Gomes / MOREIRA, Vital, *Constituição da República Portuguesa Anotada - (Artigos 1.º a 107.º).* Volume I. 4.ª Edição. Coimbra: Coimbra Editora, 2007. ISBN 978-972-32-1462-8. p. 195.
[46] *Apud* ROQUE, Miguel Prata, *A Dimensão Transnacional do Direito Administrativo – uma visão cosmopolita das situações jurídico-administrativas*. 1ª Edição. 2014. Lisboa: AAFDL. p. 34.

independência nacional, ou seja, a «capacidade [do Estado] de se dotar das *suas próprias normas*, da sua própria ordem jurídica (a começar pela Lei Fundamental), de tal modo que qualquer regra heterónoma só possa valer nos casos e nos termos admitidos pela própria Constituição (cf. art. 8º/4)» [47]. Uma outra vertente, a externa, refere a forma como o Estado, na ordem internacional, se rege em termos de igualdade e cooperação com os demais Estados.

Atualmente as grandes limitações ao exercício da soberania pelos Estados devem-se à integração e envolvimento em organizações internacionais ou regionais – decorrente da globalização –, mediante delegação de alguns dos seus poderes soberanos em organismos supranacionais.

No entanto, a soberania dos Estados em matéria criminal tem apresentado uma maior resistência, mesmo no contexto do Direito Penal Europeu, "*onde as limitações à soberania poderiam ser mais intensas*"[48], tendo em conta o avançado estado do processo de integração, comparativamente a outras organizações internacionais. De facto, o papel da União Europeia neste campo tem-se limitado à harmonização do direito substantivo e o adjetivo ao reconhecimento mútuo de decisões estrangeiras. Não se encontrando dotada de «força punitiva soberana», a União necessita de "intermediação" pelos Estados membros[49].

Por sua vez, o ordenamento jurídico português, o artigo 6.º do Código de Processo Penal[50] (CPP), consagra o **princípio da territorialidade**.

Numa definição que podemos acolher para o âmbito do direito penal nacional e contexto de direito internacional é que o «*principio de territorialidad significa que los delitos cometidos dentro del país están sujetos a la jurisdiccicíón penal nacional. En el contexto del derecho internacional, pero también com relación al âmbito del derecho penal, se refiere al principio según el cual los Estados pueden perseguir los delitos cometidos en sus respectivos territórios*»[51].

---

[47] CANOTILHO, José Gomes / MOREIRA, Vital, *Constituição da República Portuguesa Anotada* - (*Artigos 1.º a 107.º)…,* cit., p. 197.

[48] Cf. PEREIRA, Rui Soares, *O acesso (unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticos localizados no estrangeiro* in *Prova, Verdade e Processo*. Coimbra: Almedina, 2023. ISBN 978-989-40-1291-7. pp. 393-394.

[49] Cf. *Ibidem*, cit., pp. 393-394.

[50] O Decreto-Lei n.º 78/87, de 17 de fevereiro, com as sucessivas alterações introduzidas, a mais recente (49.º versão) operada pela Lei n.º 52/2023, de 28/08.

[51] PAYER, Andrés - *El principio de territorialidad y la participación delictiva transnacional* in Revista Penal [Em linha]. N.º 53 (2024), (pp. 203-222), p.204. Disponível na internet: <URL:https://revistapenal.tirant.com/index.php/revista-penal/article/view/102>. ISSN 1138-9168. [Consultado em 08/04/2025].

Numa outra formulação, este princípio consiste na *"[a]utoridade que um Estado tem de exercer jurisdição num caso específico como resultado da localização do crime no seu próprio território. Da mesma forma, esse princípio impede que outros Estados exerçam jurisdição além do seu território e limites de fronteira*" [52].

Podemos referir, numa outra formulação que estamos certos e seguros que não será originária, que "na ausência de tratados, convenções ou tratados internacionais bem como restrições decorrentes de imunidades fundadas no direito internacional e no direito constitucional, a lei processual portuguesa é aplicável em território Português a todos os cidadãos independentemente da sua nacionalidade"[53].

Atualmente, o conceito de território assume uma "*dimensão normativa"*, «segundo a qual este funciona como mero "*título de competência*" ou "*limite de exercício*" do poder público. A autonomização de diferentes territórios deixa assim de depender de uma "*unidade física*", delineada pelas suas características naturais e geográficas. Ela passa a depender de um acordo internacional acerca dos respectivos limites»[54].

O território trata-se, então, de um elemento constitutivo fundamental do Estado, uma vez que «Se uma das suas características é a da sedentariedade (Jorge Miranda) e se o Estado é um fenómeno essencialmente espacial (Sousa, 1979, p.118), não se pode conceber um Estado nómada ou sem território, apresentando-se por conseguinte o território como um *verdadeiro pressuposto existencial do Estado* (Morais, 2017,p.28)»[55].

No essencial, diremos que o "*território*" tem sido considerado de forma unânime, como um elemento constitutivo indispensável dos Estados Modernos, permitindo a coexistência, nem sempre pacífica, de várias soberanias. Ainda assim, assume um papel central na articulação entre os diversos ordenamentos jurídicos internacionais.

A ele associado, encontramos o princípio da territorialidade que pressupõe «uma *soberania territorial*, ou seja, uma potencialidade de exercício de poder público (tendencialmente) ilimitado dentro de determinado espaço geográfico. Dentro dessas fronteiras, o poder público dispõe de liberdade para conformar livremente a sua ação –

[52] Cf. MARTÍN, Cristos Velasco San, *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*. Valencia: Tirant Lo Blanch. 2016. ISBN 978-84-9086-992-5. p. 170.
[53] ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*. 2ª Edição actualizada. Lisboa: Universidade Católica, 2008. ISBN 978-972-54-0197-2. p. 59 (anotação artigo 6.º).
[54] (ROQUE, 2014, p.41).
[55] ALEXANDRINO, José Melo, *Lições de Direito Constitucional*, volume I, 2017, pp. 113-114.

"*dimensão positiva*" (também por vezes apelidada de "*ius agendi*") e de autoridade para sustar a autoridade alheia – "*dimensão negativa*" (ou "*ius excluendi alios*")[56].

Por outro lado, sendo a **"jurisdição"** um tema central desta dissertação importa sem delongas clarificar o seu significado.

Da relação de soberania entre território, os restantes elementos constitutivos do Estado – povo e poder político – e o próprio Estado, decorre um seu (da soberania) atributo essencial, a jurisdição[57]. " *A Jurisdição, não se confundindo com a soberania, poderá coincidir com esta, pois consiste na parcela da soberania que permite que um Estado possa conformar as actuações dos privados que com ele estejam em contacto, através de mecanismos integrados no seu poder político"*[58].

Em termos conceptuais, corresponde «Em sentido amplo, "*jurisdição*" corresponde à prerrogativa de exercício de poder público, através de meios coercivos, de que gozam determinadas pessoas públicas de âmbito internacional. No plano interestadual, o conceito de "*jurisdição transnacional*" foi sempre associado ao reconhecimento de personalidade jurídica internacional de cada Estado. Dela derivava esse poder jurídico-público de ditar o Direito ("*jurisdictio*"), dentro dos limites geográfico-espaciais reconhecidos pelos demais membros da comunidade internacional. Em suma, "*jurisdição transnacional*" corresponde, assim, em sentido amplo, a uma noção jusinternacionalizada das "*atribuições*" estaduais. Cada Estado exerce "jurisdição" sobre as situações de vida que ocorrem ou fazem repercutir os seus efeitos no respetivo território porque a comunidade internacional lhe reconhece essas mesmas "atribuições", entre as quais se situam a adequada regulação normativa da vida humana quotidiana que se desenvolve em determinado espaço físico»[59].

Todavia, no plano do direito internacional, o termo pode ter dois grandes significados. O primeiro - por referência doméstica ou internacional – pode querer significar em que condições as instituições judiciais que administram a justiça em nome do povo, podem declarar o que é o direito. Nesta aceção tão importante, mostra-se necessário verificar e estabelecer os limites do alcance da jurisdição de tais instituições. No nosso ordenamento jurídico, determinados tribunais só estão autorizados a exercer jurisdição relativamente a certas matérias; relativas a um determinado espaço de tempo; em determinado local; que

[56] (ROQUE, 2014, pp. 47-48).
[57] Cf. LEITE, Inês Ferreira, *O conflito de leis penais – Natureza e Função do Direito Penal Internacional*. Coimbra: Coimbra Editora, 2008. ISBN 978-972-32-1564-9. pp. 210-211.
[58] *Ibidem*, cit., p. 212.
[59] (ROQUE, 2014, pp.1059-1060).

tenham sido apresentadas por determinados sujeitos; e cuja matéria esteja inserida na competência desse tribunal[60]. Se um determinado tribunal exceder os limites da sua jurisdição, diz-se que atua *ultra vires*, isto é para lá dos seus poderes ou excedendo-os[61].

O segundo significado refere-se ao direito de os Estados autoritariamente declararem aquilo que é o direito (dentro dos seus domínios) e como deve ser aplicado. Falamos aqui da ação normativa dos Estados, que podem (e devem) tomar em mãos diversas áreas de regulação do direito (penal, fiscal, da família, do ambiente, etc.), exercendo dessa forma a sua "jurisdição" sobre essas matérias.

Devemos ainda ter presente que não devemos confundir "*jurisdição*" com o "*exercício de poder jurisdicional*". «Se a "*jurisdição*", em sentido estrito, pode ser tida enquanto expressão de um poder de decidir, unilateralmente, sobre controvérsias jurídicas, a cargo dos tribunais estaduais (ou internacionais), não é menos verdade que em sentido amplo, ela abrange igualmente a potencialidade de exercício de poder público, através de qualquer uma das funções tradicionalmente atribuídas aos Estados e às organizações internacionais: "*função legislativa*", "*função administrativa*" e "*função jurisdicional*"[62].

Para o tema desta dissertação, importa o primeiro significado (que corresponde ao sentido estrito), focado na área de atividade dos tribunais, sede própria onde são dirimidos todos os conflitos jurisdicionais internacionais.

2.2 Escolha da jurisdição e prevenção de conflitos na União Europeia.

Na abordagem clássica baseada na soberania nacional - seguida durante todo o século XX – esta questão não era um problema. A soberania e autonomia de um Estado não podia ser coartada por outros Estados.

Houve entretanto uma evolução com o surgimento da União Europeia e estabelecimento de uma área comum de livre circulação de pessoas, serviços, capitais e mercadorias.

---

[60] Corresponde, no latim, à jurisdição *ratione temporis, ratione loci, ratione personae e ratione materiae*.
[61] Cf. SIMMA, Bruno e MULLER,Andreas Th., *Exercise and limits of Jurisdiction*, in *The Cambridge Companion to International Law*, Edited by James Crawford and Martti Koskenniemi, Assistant Editor Surabhi Ranganathan, Cambridge University Press. [Em linha]. 2012, pp. 134-157, p.135. Disponível na internet:<URL:https://www.researchgate.net/profile/Andreas-Mueller-78/publication/321376192_Exercise_and_limits_of_jurisdiction/links/60f1ad0816f9f313008b453a/Exercise-and-limits-of-jurisdiction.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19>. [Consultado em 09/04/2025].
[62] (ROQUE, 2014, pp.1063-1064).

Foi, pois, com naturalidade que assistimos a um aumento da criminalidade transnacional, originando situações em que múltiplos Estados seriam, simultaneamente, competentes para investigar e punir condutas (jurisdições concorrentes).

Por conseguinte, foram inevitáveis as consequências com impacto a nível da soberania, disposições legais jurisdicionais e boa administração da justiça e difíceis as tentativas de estabelecimento de regras comuns para resolução dos conflitos de jurisdições.

Pese embora, como referimos, os Estados tenham a prerrogativa de poder estabelecer jurisdição, inclusive, relativamente a crimes cometidos pelos seus cidadãos no estrangeiro (jurisdição extraterritorial), contudo, já não poderá conduzir investigações nem tão pouco impor as respetivas penas no estrangeiro (competência jurisdicional de aplicação e cumprimento)[63].

O conselho da Europa, cedo reconheceu que os conflitos de jurisdição poderiam ter um impacto negativo na boa administração da justiça e pese embora tenha manifestado essa preocupação no preâmbulo da Convenção Europeia sobre a Transferência de Processos em Matéria Penal[64], a verdade é que não resolveu de forma adequada todos os conflitos de jurisdição. Ao permitir que um Estado transfira a sua competência para outro Estado, cria um novo espaço de jurisdição nesse Estado (o recetor). A esse respeito devemos ter em consideração os artigos 2 e 7. Por outro lado, as disposições da convenção podem ajudar a reduzir os problemas de conflitos de jurisdição em todos aqueles casos em que os países requerentes/recetores podem atuar de acordo com as suas próprias disposições legais jurisdicionais (cf. artigos 7 e 8).

Significativo viria a ser, entretanto, o trabalho desenvolvido pela União Europeia (UE). A partir de 1997, uma das suas competências passou a ser, precisamente, a prevenção de conflitos de jurisdição no domínio da cooperação judiciária em matéria penal (o antigo terceiro pilar). Após o Tratado de Lisboa, as disposições relevantes

---

[63] PANZAVOLTA, Michele, *Choosing the National Forum in Proceedings Conducted by the EPPO: Who Is to Decide?* in WINTER, Lorena Bachmaier, *The European Public Prosecutor's Office: The Challenges Ahead - Legal Studies in Internacional, European and Comparative Criminal Law 1*. Volume I. Cham, Switzerland: Springer Nature Switzerland AG, 2018 (pp. 59-83). ISBN 978-3-319-93915-5. pp. 60-61.

[64] O passo mais significante, a Convenção Europeia sobre a Transferência de Processos em Matéria Penal (*European Convention on the Transfer of Proceedings in Criminal Matters*), que no preâmbulo refere "*Considerando que é útil assegurar, num espírito de confiança mútua, a organização dos procedimentos processuais penais a nível internacional, em particular, evitando, os inconvenientes resultantes dos conflitos de competência*,", tradução nossa. Disponível na internet:<URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680072d42>. [Consultado em 09/04/2025].

encontram-se nos artigos 82.º a 86.º do Tratado sobre o Funcionamento da União Europeia (TFUE)[65] no âmbito do qual, o artigo 82.º, n.º 2 conferiu à UE (Parlamento e Conselho Europeu) poderes para não só adotar medidas preventivas, mas também resolver conflitos de jurisdição.

Em 2009, poucos meses antes da entrada em vigor do Tratado de Lisboa, a UE aprovou a Decisão-Quadro 2009/948/JAI[66] para abordar diretamente os conflitos de jurisdição. De acordo com esta Decisão-Quadro, deve existir troca de informações entre os Estados-Membros sempre que houver motivos razoáveis para acreditar que decorrem processos paralelos. Neste cenário, devem consultar-se reciprocamente, com o objetivo de encontrar uma solução adequada para a gestão do conflito. A solução pode passar por, mas não tem forçosamente de ser, a concentração dos processos penais num único Estado-Membro[67]. Com este propósito, o artigo 12 da Decisão-Quadro atribuiu formalmente à Eurojust um papel coordenador (para os casos sob alçada da sua competência), no sentido de facilitar a cooperação judicial entre os Estados-Membros da UE. No âmbito dos conflitos de jurisdição, este organismo desempenha um papel consultivo (de aconselhamento), ajudando os Estados a encontrar soluções para questões relacionadas com conflitos de jurisdição. Encontramos uma menção expressa desse papel na Decisão Eurojust[68].

De acordo com a Decisão do Conselho 2009/426/JAI de 16 de dezembro de 2008, relativa ao reforço do Eurojust (que alterou a Decisão 2002/187/JAI de 28 de fevereiro de 2002), os Estados-Membros asseguram que os seus membros nacionais Eurojust sejam

---

[65] TFUE disponível na internet: <URL:https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>. [Consultado em 09/04/2025].

[66] Decisão-Quadro 2009/948/JAI de 30 de Novembro de 2009 relativa à prevenção e resolução de conflitos de competência em processo penal [2009] JO L328/42. Disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009F0948>. [Consultado em 10/04/2025].

[67] Críticas à falha da Decisão-Quadro 2009/948/EU em criar uma verdadeira área de liberdade, segurança e justiça referem a ausência de um mecanismo vinculativo para os Estados-Membros, são expressas por VERVAELE, John A.E., *European criminal justice in the post-Lisbon area of freedom, security and justice*. [Em linha]. (2014), pp. 1-312, p. 287. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://core.ac.uk/download/pdf/150084157.pdf>. [Consultado em 21/04/2025].

[68] Decisão do Conselho 2002/187/JAI de 28 de fevereiro de 2002 relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade [2002] JO L063 (pp. 0001-0013), com as alterações introduzidas pela Decisão do Conselho 2009/426/JAI de 16 de dezembro de 2008, relativa ao reforço da Eurojust e que altera a Decisão 2002/187/JAI relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade [2009] JO L138/14 (pp. 14-32).
Disponíveis na internet:
<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002D0187> e <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009D0426>. [Consultado em 10/04/2025].

informados dos casos em que tenham surgido ou possam surgir conflitos de jurisdição (artigo 13.º, n.º 7, al.a)). Além disso, estabelece o artigo 7.º, n.º 2 que " *Se dois ou mais membros nacionais não conseguirem chegar a acordo para resolver um caso de conflito de jurisdição quanto à realização de uma investigação ou ao início de um procedimento penal […], o Colégio é convidado a emitir um parecer escrito não vinculativo sobre o caso, na condição de o problema não poder ser solucionado por acordo entre as autoridades nacionais competentes em questão. O parecer do Colégio é transmitido sem demora aos Estados-Membros envolvidos […]*."

Apesar destes instrumentos legais representarem um passo significativo na tentativa de resolverem questões relacionadas com conflitos de competência, a verdade é que a UE ainda não dispõe de um sistema que atribua, de forma vinculativa, competências criminais nem tão pouco de um mecanismo vinculativo de resolução de conflitos jurisdicionais. Os Estados não podem ser obrigados a instaurar processos, a evitar a sua instauração ou a arquivá-los. As prerrogativas da soberania nacional permanecem, neste aspeto, praticamente inalteradas.

2.2.1 *O princípio ne bis in idem*

O único mecanismo com força vinculativa relativo ao exercício de poder jurisdicional dos Estado, é o princípio *ne bis in idem*. Este princípio encontra-se ínsito no artigo 54.º da Convenção de Aplicação do Acordo Schengen de 14 de Junho de 1985 (JO L 239, pp. 19-62)[69] e no art.º 50.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE)[70]. Tendo um Estado exercido Jurisdição positiva, decidindo um caso com base no mérito da causa, os outros Estados ficam impedidos de instaurar novos processos. Embora vinculativo, o princípio não é absoluto, pois está sujeito a limites e exceções. Primeiro, o princípio *ne bis in idem* do artigo 54.º da Convenção Schengen só é despoletado nos casos em que tenha existido uma condenação, a pena tenha sido cumprida ou esteja atualmente em curso de execução ou não possa já ser executada, segundo a legislação da parte contratante em que a decisão de condenação foi proferida (*enforcement condition*). Em segundo lugar, o princípio não impede a existência (simultânea) de

[69] Disponível na internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:42000A0922(02)>. [Consultada em 10/04/2025].
[70] Disponível na internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT>. [Consultada em 10/04/2025].

duplicação de processos (*lis pendens*). Em terceiro, o artigo 55.º da Convenção Schengen permite que as partes contratantes, nos casos ali identificados, excecionem a aplicação do artigo 54.º e vários países aproveitaram essa possibilidade. Este princípio, não se mostra, portanto, adequado a resolver questões relacionadas com conflitos de jurisdição. Ademais, este princípio opera numa lógica de "primeiro a chegar, primeiro a ser atendido", que pode induzir a comportamentos competitivos inadequados por parte das autoridades nacionais. Na verdade, elas podem sentir-se pressionadas a agirem o mais depressa possível no sentido de garantirem a execução da sua sentença.

O panorama geral é que a questão dos conflitos de jurisdição ainda está, em grande parte, deixada ao critério e vontade dos Estados-Membros no sentido de encontrarem soluções comuns, ficando o princípio *ne bis in idem* a atuar numa instância final (nos casos em que o princípio possa ser aplicado).

Neste contexto, anteriormente já havíamos referido que uma das grandes limitações ao exercício da soberania pelos Estados deve-se ao envolvimento e integração em organizações internacionais.

O estabelecimento do *European Public Prosecutors´s Office* (EPPO)[71] acabou por ser um marco na forma como os países europeus passaram a lidar com as investigações lesivas dos interesses económicos da UE.

A questão que naturalmente se coloca, e sobre a qual tentaremos dar resposta, será, como é que a EPPO lida e aborda questões relacionadas com conflitos de jurisdição.

2.3 A Jurisdição na EPPO

O TFUE dispõe no artigo 86.º, n.º 1, "*A fim de combater as infrações lesivas dos interesses financeiros da União, o Conselho, por meio de regulamentos adotados de acordo com um processo legislativo especial, pode instituir uma Procuradoria Europeia a partir da Eurojust. O Conselho delibera por unanimidade, após aprovação do Parlamento Europeu*". O parágrafo seguinte clarifica que "*A Procuradoria Europeia é competente para investigar, processar judicialmente e levar a julgamento, eventualmente em articulação com a Europol, os autores e cúmplices das infrações lesivas dos interesses financeiros da União determinadas no regulamento a que se refere o n.º 1. A*

[71] A Procuradoria Europeia foi formalmente reconhecida com o Tratado de Lisboa. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>. [Consultado em 10/04/2025].

Procuradoria Europeia exerce, perante os órgãos jurisdicionais competentes dos Estados-Membros, a ação pública relativa a tais infrações".

As competências materiais da Procuradoria Europeia estão reguladas no artigo 86.º, n.º 2 do TFUE, que estabelece "*A Procuradoria Europeia é competente para investigar, processar judicialmente e levar a julgamento, eventualmente em articulação com a Europol, os autores e cúmplices das infrações lesivas dos interesses financeiros da União determinadas no regulamento a que se refere o n.º 1. A Procuradoria Europeia exerce, perante os órgãos jurisdicionais competentes dos Estados-Membros, a ação pública relativa a tais infrações*". Para melhor compreensão desta atribuição, devemos considerar o anterior artigo 86.º, n.º 1 bem como o artigo 325.º do TFUE que impõe em particular, uma obrigação geral de combate às fraudes e quaisquer outras atividades ilegais lesivas dos interesses financeiros da União (todas as receitas, despesas e ativos cobertos por, adquiridos através de ou devidos ao orçamento da União, aos orçamentos das instituições, dos órgãos e dos organismos da União criados nos termos dos Tratados, ou os orçamentos por eles geridos e controlados direta ou indiretamente), por meio de medidas que tenham um efeito dissuasor e proporcionem uma proteção efetiva nos Estados-Membros, bem como nas instituições, órgãos e organismos da União. Na definição e tipificação dos crimes que seriam suscetíveis de lesar os interesses financeiros da União, os Estados membros, para evitarem a regra de unanimidade prevista no artigo 86.º do TFUE, decidiram, por uma questão de coerência, utilizar instrumentos jurídicos já existentes, que definem esses atos criminosos de forma harmonizada: Nestes termos, as competências do Organismo poderiam ser indiretamente alteradas, alterando a definição dos crimes contra os interesses financeiros da União Europeia (crimes PIF como definidos na Diretiva (EU) 2017/1371[72] - Diretiva PIF). Isso implicaria a submissão dessas alterações no âmbito de um processo legislativo ordinário, que não exige unanimidade. Por conseguinte, a competência da Procuradoria Europeia baseia-se numa definição destes comportamentos por referência à Diretiva PIF, que descreve estes atos para efeitos de harmonização, ainda que estes venham a ser implementados pela legislação nacional de cada um dos Estados membros. Tal referência é, por conseguinte, dinâmica: se a Diretiva PIF mudar no futuro, isso teria impacto indireto na competência da Procuradoria Europeia.

[72] Diretiva (UE) 2017/1371 do Parlamento Europeu e do Conselho de 5 de julho de 2017 relativa à luta contra a fraude lesiva dos interesses financeiros da União através do direito penal publicado no JO 28.7.2017, L 198/29. Disponível na internet: <URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017L1371>. [Consultado em 21/04/2025].

Todavia, para o que importa neste estudo, o TFUE não clarifica o significado de órgãos jurisdicionais competentes. Por esse motivo, cabe à legislação secundária (Lei), definir tal conceito. De acordo com o artigo 86.º, n.º 3 do TFUE, "*Os regulamentos a que se refere o n.º 1 definem o estatuto da Procuradoria Europeia, as condições em que esta exerce as suas funções, as regras processuais aplicáveis às suas atividades e as que regem a admissibilidade dos meios de prova, bem como as regras aplicáveis à fiscalização jurisdicional dos atos processuais que a Procuradoria Europeia realizar no exercício das suas funções*".

O Tratado deixa sem resposta a questão dos conflitos de jurisdição. Qual deve ser a jurisdição nacional competente para determinado processo? Deverá a regulamentação europeia abranger questões relacionadas? E, em caso afirmativo, como proceder?

A complicar ainda mais, o desenho (em dupla camada), que conforma e caracteriza a estrutura dos procedimentos conduzidos pela Procuradoria Europeia, de acordo com as regras estabelecidas pelo Tratado: uma fase de investigação europeia (realizada por procuradores europeus) e uma fase de julgamento nacional (a cargo dos tribunais nacionais). O problema da escolha do foro diz respeito à identificação do país onde irá decorrer o julgamento. No entanto, pode incluir a fase de investigação, a menos que o Regulamento Europeu consiga estabelecer uma investigação totalmente europeia inteiramente regida pelas regras europeias e revista pelos tribunais europeus. Como veremos, este não foi o caso.

Caso o problema da escolha da jurisdição se estenda à escolha do local da investigação, surgem novas questões. Qual ou quais os tribunais e de que países, devem ser competentes para emitir um mandado de prisão ou para autorizar certas medidas de investigação? A questão torna-se ainda mais premente caso não venha a existir harmonização das regras nacionais relativas aos poderes de investigação, ou caso esta se revele insuficiente. E como devem interagir as competências relativas à investigação e julgamento? Por fim, deve o procurador ter o poder de escolher onde o caso será investigado ou não? Estas questões são avançadas por PANZAVOLTA[73].

Pouco tempo depois da adoção do Tratado de Lisboa, começou o debate relativo às regras do Regulamento que viria estabelecer a EPPO. Foi em 2013 que a Comissão finalmente apresentou uma proposta de Regulamento. Após um longo período de discussões e negociações, o texto foi finalmente aprovado em 2017.

[73] (PANZAVOLTA, 2018, p.64).

Durante o processo negocial, as regras acerca da jurisdição passaram por alterações significativas. Vejamos como ficaram estabelecidas.

2.3.1 EPPO – Regras relativas à jurisdição

No texto final adotado, o artigo 26.º do Regulamento (UE) 2017/1939 do Conselho de 12 de outubro de 2017[74] define as regras relativas à escolha da jurisdição e teve em conta algumas das críticas formuladas durante o processo negocial[75]. Na proposta do Conselho da União Europeia de 12 de junho de 2015[76], em nota de rodapé (nt.78), fez-se constar que a "*HU e SK gostariam de acrescentar critérios adicionais, em particular nas relativas à localização da prova. PL prefere seguir o modelo contante em bases de modelos de jurisdição de outros instrumentos de direito penal da UE, onde a "residência habitual" está ausente ou - no máximo - é opcional - motivo pelo qual, não há razão para que figure em primeiro lugar na ordem de prioridade. Ver, por exemplo, a Diretiva 2001/93 e a Diretiva 2013/40*" (tradução nossa).

De acordo com o texto final do regulamento aprovado (UE 2017/1939 do Conselho de 12 de outubro de 2017), o artigo 26.º, n.º 4, dispõe "*Em princípio, o processo é aberto e instruído por um Procurador Europeu Delegado do Estado-Membro onde está centrada a atividade criminosa ou, caso tenham sido cometidas várias infrações conexas abrangidas pelas competências da Procuradoria Europeia, do Estado-Membro em que foi cometida a maior parte das infrações Um Procurador Europeu Delegado de outro Estado-Membro que tenha competência para conhecer do processo só pode abrir uma investigação ou receber instruções para o fazer da Câmara Permanente se o desvio da regra estabelecida no período anterior for devidamente justificado com base nos seguintes critérios, por ordem de prioridade: a) O local de residência habitual do suspeito ou do arguido; b) A nacionalidade do suspeito ou do arguido; c) O local onde ocorreu o principal prejuízo financeiro.*"

A decisão sobre a escolha do foro recai sobre as competentes Câmaras Permanentes com base em relatório (e projeto de decisão) do competente Procurador Europeu Delegado (artigo 10.º, n.º 3 e n.º 4 do Regulamento). A este respeito ter em conta, em

[74] Regulamento (UE) 2017/1939 do Conselho de 12 de outubro de 2017 que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia. Disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32017R1939>. [Consultado em 10/04/2025].
[75] A redação final do artigo 26 foi sensivelmente modificada quando comparada com a versão anterior da proposta de texto negociada em junho de 2015 (Conselho doc. N.º 9372/15, Brussels, 12 Junho 2015).
[76] Disponível na internet:<URL:https://data.consilium.europa.eu/doc/document/ST-9372-2015-INIT/pt/pdf>. [Consultada em 11/04/2025].

particular, as alíneas a) e e) do artigo 10.º, n.º4 e ainda o Considerando 87, ambos do Regulamento. De acordo com o artigo 10.º, n.º 9, o Procurador Europeu não tem direito a voto nas decisões da Câmara Permanente. A intenção parecer ter sido excluir qualquer tipo de parcialidade que pudesse existir por parte do Procurador Europeu supervisor em relação à prossecução (ou não) do processo no seu Estado-Membro.

As alterações relativas a proposta então apresentada pelo Conselho foram significativas e encaminhadas no sentido de existir por parte dos instrumentos legais europeus uma identificação mais precisa do *forum* nacional, aliás, como havia sido, explicitamente, requerido pelo Parlamento Europeu.

As disposições finais adotadas tomam o *locus commissi delicti* como ponto de partida. O local da prática do crime torna-se o parâmetro principal. Outros critérios - subsidiários - foram adicionados de acordo com uma ordem de prioridade clara. O texto adotado denota uma preocupação acrescida com a previsibilidade do foro onde o processo virá a decorrer.

Os outros critérios suplementares também sofreram alterações. Em primeiro lugar, além do local de residência do suspeito, o novo texto introduziu a nacionalidade do suspeito. Na parte que se revelaria de grande interesse para esta dissertação, o artigo 26.º do Regulamento eliminou o critério da localização da prova, na medida em que teria levantado grandes dificuldades de aplicação prática em todos aqueles casos em que a prova estivesse localizada em mais de um país ou onde fosse difícil estabelecer com precisão a localização geográfica da prova (por exemplo, dados de computador armazenados na nuvem).

Deixou de existir referência ao local de residência das vítimas diretas. Tal disposição acabou por ser considerada ilógica no âmbito do contexto de crimes em que a principal vítima acaba por ser a União. O critério foi substituído pelo local onde ocorre o maior prejuízo financeiro.

Devemos observar também que, de acordo com o Artigo 26.º do Regulamento, a escolha do país é feita numa fase prévia do processo. Ao contrário da proposta da Comissão e de anteriores projetos, as regras relativas à seleção do foro nacional estão agora incluídas na parte relativa ao início da investigação - e, portanto, tornam-se plenamente aplicáveis já na fase inicial do processo. No entanto, isto não é tanto o sinal de uma maior preocupação com o princípio do juiz natural. É sobretudo a consequência de uma reestruturação (durante as negociações no Conselho) da organização da EPPO mais de acordo com uma conceção tradicional baseada no conceito da soberania nacional.

Existe, de facto, um compromisso entre a centralização dos procedimentos a nível europeu e o momento processual da escolha do foro nacional. Se a EPPO for chamada a intervir no âmbito de um espaço jurídico único, onde as divisões entre os Estados-Membros são superadas (princípio da territorialidade europeia), a escolha antecipada do foro nacional torna-se menos importante. Um cenário desse tipo, por sua vez, exige que as normas substantivas e processuais entre os Estados-Membros sejam harmonizadas de uma forma mais significativa e, ainda, que o controle judicial da fase de investigação esteja centralizado a nível europeu. Perante um cenário com este paradigma, seria razoável que um procurador europeu submetesse os casos perante um tribunal europeu, em detrimento de um tribunal nacional. Por outro lado, caso não exista uma área jurídica única durante as investigações, e a divisão de soberania entre os países permanecer (com as subsequentes diferenças nas regras aplicáveis), a escolha antecipada do foro nacional torna-se essencial (com o controle judicial e as autorizações no âmbito da fase de investigação a poderem permanecer a nível nacional). A norma final adotada acabou por ser um sinal dessa mudança de perspetiva.

A ideia do procurador europeu, durante as investigações, poder atuar numa lógica de área jurídica comum, sem fronteiras, foi abandonada durante as negociações. O compromisso - sem surpresa - foi na direção de uma maior proteção das prerrogativas de soberania. Mesmo na fase de investigação, as fronteiras nacionais permaneceram presentes e intactas, com os procuradores europeus a terem de atuar em limites territoriais precisos, recorrendo à cooperação do Procurador Europeu Delegado assistente do respetivo País em que se venha a justificar proceder à recolha de prova. O Regulamento aprovado (Regulamento (EU) 2017/1939, de 12 de outubro de 2017), de facto, estabelece uma clara distinção entre o "Procurador Europeu Delegado competente" e o "Procurador Europeu Delegado assistente" (ver Artigo 2.º, n.º 6). O primeiro é responsável pela investigação e acusação de um caso específico. Cada caso é, portanto, atribuído a um Procurador Europeu Delegado competente, responsável pelas investigações e ações penais, que atua nos limites da sua jurisdição nacional. Para atividades transfronteiriças, deve recorrer ao Procurador Europeu Delegado assistente do Estado onde o ato deva ser praticado ou a medida deva ser adotada (ver Artigo 31.º).

Essencialmente, o Regulamento confirma o atual estado de fragmentação das investigações transfronteiriças entre países, mas estruturou a Procuradoria Europeia para que esta tenha ramificações em todos os Estados-Membros: esta estrutura deve permitir que a EPPO atue - o mais rapidamente possível - entre jurisdições e minimizar os

problemas práticos relacionados com a atuação em diferentes jurisdições. Este desenho, acabou por proteger as prerrogativas dos Estados nacionais no que diz respeito à administração da justiça penal, sendo facilmente percetível, a razão pela qual colheu a preferência da grande maioria dos países negociadores. Tal arranjo, no entanto, aumenta a importância da escolha do país do Procurador Europeu Delegado competente, pois as regras aplicáveis dependerão em grande medida dessa escolha.

Outras questões se levantam, nomeadamente, as relacionadas com a validade da prova obtida em contexto transnacional, que não abordaremos. Deixamos aqui apenas uma breve nota a este respeito, que assume a maior relevância no sentido de aferir à luz de que ordem jurídica deverá ser apreciada a admissibilidade e legalidade da utilização de determinado meio de prova, nomeadamente, aquela cuja recolha seja efetuada mediante o recuso a métodos ocultos de investigação criminal.

Deixaremos de seguida uma breve referência aos mecanismos de cooperação judiciária, à proposta de Directiva do *European Law Institute* (ELI) e à importância que se pode vir a revestir o *e-Evidence Digital Exchange System* (e-EDES) e nível europeu.

2.4 Os mecanismos de cooperação judiciária, proposta de Directiva de reconhecimento mútuo de admissão de prova transfronteiriça e o *e-Evidence Digital Exchange System (e-EDES)*.

No âmbito da justiça penal, acontece por vezes, que os Estados necessitam da colaboração de outros Estados para o exercício do *jus puniendi*. Para o efeito, o Estado pede (roga) a outro Estado que lhe providencie assistência para prossecução num processo em curso no Estado requerente, isto é, pedindo, em função de cada situação específica, a colaboração de outro Estado (o rogado), sob a forma de cooperação que melhor se ajuste ao caso em concreto e ao que é pretendido pelo Estado requerente (rogante).

No contexto de cooperação judiciária internacional coexistem modalidades de pedidos solenes, complexos e formais, como sejam os pedidos e processos de extradição, com outras modalidades menos solenes, mas de reconhecida importância no âmbito de investigações criminais transnacionais, como sejam os pedidos de auxílio (assistência) judiciário mútuo, onde encontramos uma diversidade de medidas (*v.g.* pedidos de

notificação e audição de testemunhas, de suspeitos e peritos, apreensões, exames e perícias, informações relativas a contas e movimentações bancárias)[77].

O regime legal aplicável ao auxílio mútuo assentava, até muito recentemente, sobretudo em Convenções e Protocolos, quer do Conselho da Europa (CoE) — Convenção Europeia de Auxílio em Matéria Penal de 1959[78] e Protocolos — quer da própria UE — Convenção de 2000 sobre o Auxílio Judiciário Mútuo em Matéria Penal[79], Protocolo, e Convenção de Aplicação do Acordo de Schengen (CAAS)[80] — e isto se apenas nos quisermos referir ao regime aplicável no espaço da UE e, assim, também em Portugal. Estes instrumentos previam já uma obrigação dos Estados concederem mutuamente um amplo auxílio judiciário (artigo 1.º, n.º 1, da Convenção de 1959 do CoE) e previam já o envio direto de pedidos entre autoridades judiciárias (divergindo do clássico auxílio judiciário que era realizado entre Estados através de processos morosos), regendo-se ainda pelo modelo do pedido acima descrito.

Assim, os artigos 82º a 86.º do TFUE abordam aspetos relacionados com a cooperação judiciária em matéria penal, com especial ênfase no princípio do reconhecimento mútuo de sentenças e decisões judiciais, incluindo a aproximação das disposições legislativas e regulamentares dos Estados-Membros nos domínios relativos a matéria penal sempre que se afigure indispensável para assegurar a execução eficaz das políticas da União. Já aqui abordamos o papel coordenador do Eurojust no sentido de uma aproximação entre os Estados-Membros em matéria de cooperação, tendo esta entidade, de acordo com o artigo 85.º, n.º 1, alíneas a), b) e c) do TFUE as seguintes funções: "*a) A abertura de investigações criminais e a proposta de instauração de ações penais conduzidas pelas autoridades nacionais competentes, em especial as relativas a infrações lesivas dos interesses financeiros da União; b) A coordenação das investigações e ações penais referidas na alínea a); c) O reforço da cooperação judiciária, inclusive mediante a resolução de conflitos de jurisdição e uma estreita cooperação com a Rede Judiciária Europeia*". Por sua vez, o artigo 85.º, n.º 2 refere "*No âmbito do exercício das ações*

[77] Artigo 145.º da Lei n.º 144/99, de 31 de Agosto, Lei da Cooperação Judiciária Internacional em Matéria Penal. Disponível na internet:<URL:https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=295A0145A&nid=295&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo>. [Consultada em 22/04/2025].
[78] Disponível na internet:<URL:https://dcjri.ministeriopublico.pt/instrumento/convencao-europeia-de-auxilio-judiciario-mutuo-em-materia-penal-1>. [Consultado em 22/04/2025].
[79] Disponível na internet:<URL:https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/63-2001-626203>. [Consultado em 22/04/2025].
[80] Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:42000A0922(02)>. [Consultado em 22/04/2025].

penais a que se refere o n.º 1 e sem prejuízo do artigo 86.º, os atos oficiais de procedimento judicial são executados pelos agentes nacionais competentes", ou seja, em momento algum se prevê a ingerência de um Estado noutro Estado, mas apenas a cooperação a nível europeu.

Breve referência ainda a este respeito, à CBCc que veio uniformizar conteúdos e trazer uma mais-valia a nível da cooperação judiciária, em especial com a criação da Rede 24/7. Esta rede assegura um contacto permanente entre os países subscritores da Convenção, 24 horas por dia, 7 dias por semana. Através desta rede e mediante utilização de meios expeditos, poderá ser efetuado pedido de preservação expedita de dados, informação sobre assinantes de IP ou outras diligências pertinentes. Por força do artigo 21.º da LCc em Portugal o ponto de contacto ficou sob a alçada da Polícia Judiciária.

As investigações que cuidamos nesta dissertação, como vimos, podem ter contatos com diversos países. Perante este tipo de criminalidade informática sem fronteiras e volatilidade dos elementos de prova que possam existir, a atuação os OPC e autoridades judiciárias exige, por conseguinte, rapidez de atuação.

Certo é que até recentemente ainda não se havia logrado avançar sobre uma proposta legislativa relativa à admissão da prova transfronteiriça. Tanto a Directiva 2014/41/EU, de 03 de abril de 2014, relativa à decisão europeia de investigação em matéria penal, como o Regulamento (UE) 2017/1939 do Conselho, apesar de disporem algumas regras isoladas destinadas a facilitar a admissão de provas transfronteiriças, nenhum deles dispõe acerca dos princípios aplicáveis a este respeito nem tão pouco relativamente à possibilidade de exclusão da prova[81].

Neste sentido, pela relevância, merece destaque a proposta de Diretiva apresentada em 05 de maio de 2023 pelo *European Law Institute* (ELI)[82]. Em termos sucintos, surgiu no seguimento de um projeto do programa justiça da UE (2020-2023), que visou

---

[81] SANTOS, Antonio Martínez, *Admisibilidad Mutua de Prueba Penal Transfronteiriza en la Unión Europea: La Propuesta de Directiva Del European Law Institute* in *Revista General de Derecho Procesal*, N.º 61. 2023. ISSN 1696-9642. p.3.
Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Admissibility_of_E-Evidence/426388-1.pdf>. [Consultado em 20/05/2025].

[82] WINTER, Lorena Bachmaier, SALIMI, Farsam, RAMOS, Vânia Costa [*Et. al*], *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings – Draft Legislative Proposal of the European Law Institute.* Vienna: European Law Institute, 2023. ISBN 978-3-9505318-6-2.
Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>. [Consultada em 20/05/2025].

providenciar um guia para a legislação futura da UE (artigo 82.º do TFUE – princípio do reconhecimento mútuo na cooperação judiciária em matéria penal) e apresentação de um *draft* de proposta legislativa com padrões comuns de admissão de prova e prova electrónica transfronteiriça. É importante destacar que a proposta define os conceitos de «prova» e «prova electrónica» para efeitos de admissibilidade, em termos muito amplos[83]. Esta proposta encontra-se dividida em três partes: a primeira (Capítulo 2, artigos 4.º a 6.º) contém normas que pretendem fixar as regras que devem ser respeitadas nos processos penais em que existam provas obtidas noutro EM diferente, ou seja, aquelas que foram obtidas de acordo com normas e princípios, provavelmente, diferentes dos aplicáveis no estado do foro. Convém salientar, que a proposta não contém disposições relativas aos procedimentos e regras de recolha de prova, não estipula a forma como são reguladas as medidas de investigação dos EM e também não se refere à livre apreciação e valoração da prova, a cargo dos Tribunais nacionais; a segunda parte (Capítulo 3, artigos 7.º a 9.º) propõe um conjunto de normas específicas em matéria de admissibilidade das provas electrónicas, estabelecendo regras precisas de recolha e transmissão da prova digital, por forma a assegurar a sua integridade e autenticidade[84]; a terceira (Capítulo 4) afere relativamente à preparação dos recursos legais e medidas eficazes que permitam à defesa contestar sentenças proferidas com base em provas que tenham sido admitidas com base na violação das disposições da proposta de Directiva[85].

Os critérios reconhecidos na primeira parte da proposta conjugam os dois principais interesses em jogo: a salvaguarda dos direitos dos arguidos e a promoção da circulação de provas na UE. Com este propósito, o artigo 4.º da proposta estabelece como princípio fundamental o *locus regit actum*. De acordo com o n.º 1, deste artigo 4.º, os EM garantem que as provas obtidas em conformidade com as normas do EM de origem (*lex loci*) podem ser utilizadas nos processos penais do EM do foro[86]. Por outras palavras, procura-se assegurar que a recolha de prova é feita de acordo e em conformidade com a *lex loci*,

[83] (SANTOS, 2023, p. 4).
[84] Baseadas sobretudo em *standards* forenses internacionais constantes do documento *The Global Guidelines for Digital Forensics Laboratories de Interpol de 2019*, disponível na internet:<URL:https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics>. [Consultado em 21/05/2025].
[85] ORLANDO, Claudio, *Mutua Ammissibilità Della Prova Tra Gli Stati Membri DellÚnione Europea Ed E-Evidence: Riflessiooni a Margine Della Proposta Di Direttiva Dello European Law Institute* in *Sistema Penale (SP)*. 11/2023. ISSN 2704-8098. (pp. 19-33), p.24. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sistemapenale.it/fascicoli/1701360858_fasc-112023.pdf>. [Consultado em 20/05/2025].
[86] (SANTOS, 2023, p. 6).

sendo que o controlo é assegurado pelo Tribunal do julgamento (reforçando o respeito pelos direitos dos arguidos) e também que as provas obtidas mediante regras diferentes da *lex fori* não conduzem à sua inadmissibilidade a menos que sejam violados princípios fundamentais do Estado do foro (aumentando a livre circulação de provas e eficácia dos processos transfronteiriços). O cumprimento da *lex loci* acaba por ter uma dupla função: por um lado, opera como requisito de admissibilidade das provas no Estado do foro; por outro lado, serve para garantir que a diversidade de ordenamentos jurídicos não irá representar um obstáculo para a admissão de provas obtidas no estrangeiro[87].

Desta forma o princípio geral de admissibilidade da prova em procedimentos transnacionais acabou por ser reconhecido no Capítulo 2 da proposta, onde se estabelecem as regras gerais que os EM devem respeitar nos casos em que a prova foi recolhida noutro país. Tratou-se, sem dúvida, de um grande esforço encetado pelo legislador europeu, especialmente se tivermos em consideração toda esta nova tipologia de provas – provas electrónicas – muitas delas com diversos contactos transfronteiriços uma vez que as informações e dados recolhidos podem estar armazenados em países terceiros, com diferentes disposições legais relativamente aquele onde a prova será utilizada[88]. A questão que logicamente se coloca é qual é a *lex loci* aplicável a estas provas electrónicas em que se desconhece a sua localização. O artigo 3.º, alínea d) da proposta clarifica esta questão, definindo a *lex loci* nestes casos «como a do lugar onde se teve acesso à prova electrónica», independentemente da localização física do suporte ou servidor em que esta se encontre armazenada[89].

Esta proposta tem sido considerada como um valioso contributo para o futuro da cooperação judiciária em matéria penal, cada vez mais caracterizada por uma dimensão transnacional. Esta intervenção, considerada significativa, uma vez que para além das normas comuns de admissibilidade de reconhecimento de provas entre EM, também disciplina e salvaguarda os direitos fundamentais e garantias de participação dos visados pelos procedimentos de recolha de prova, evitando que esta natureza transfronteiriça possa vir a ter um impacto negativo no que são os direitos dos arguidos. O envolvimento da defesa nos procedimentos de recolha de prova transnacional – em particular as provas electrónicas – mitiga eventuais situações patológicas que possam vir a surgir no processo

[87] *Ibidem*, cit., p. 7.
[88](ORLANDO, 2023, p.5).
[89] (SANTOS, 2023, p. 7). Autor refere, certamente, por lapso, o artigo 2.º da proposta.

e nesse sentido só valoriza a proposta que se espera possa vir a ser seguida de uma iniciativa legislativa por parte da Comissão Europeia[90].

É também neste plano que se nos afigura de extrema importância o *e-Evidence Digital Exchange System* (e-EDES)[91], ainda em fase piloto, motivo pelo qual a informação a este respeito será meramente indicativa.

A Comissão Europeia, baseada nas Conclusões do Conselho da UE de 9 de Junho de 2016 sobre a melhoria da justiça penal no Ciberespaço, lançou através da DG JUST (*Directorate-General for Justice AND Consumers*) um projeto para construir e-EDES, consistindo numa plataforma de comunicação eletrónica segura para agilizar as trocas de provas entre as autoridades judiciárias competentes dos Estados Membros no âmbito da Decisão Europeia de Investigação (DEI)[92] e outros instrumentos de auxílio judiciário mútuo em matéria penal.

O funcionamento do sistema (plataforma) visa viabilizar e assegurar a troca eletrónica segura dos dados da cooperação judiciária em matéria penal (emissão e receção eletrónica das DEI e cartas rogatórias) com um grande número de autoridades judiciárias (AJ) de Estados Membros da UE.

Ainda em fase piloto, a participação no e-EDES assume cariz voluntário, mas a CE estima que este sistema venha a ser usado por grande parte das AJ de todos os Estados membros e que em 2025 seja obrigatório para todas as AJ da UE, na sequência dos procedimentos legislativos em curso no Parlamento Europeu e no Conselho com vista à aprovação de uma Diretiva e um Regulamento sobre a matéria[93].

Com o portal e-EDES será possível às AJ preparar os formulários da DEI e cartas rogatórias de forma digital e enviá-los como mensagem à autoridade competente para a execução. A importância que atribuímos a este portal está diretamente relacionado com a sugestão que aqui deixamos, da possibilidade de, por esta via, as pesquisas informáticas

---

[90] (ORLANDO, 2023, p.33) e no mesmo sentido (SANTOS, 2023, p. 13).

[91] Relativamente a aspetos técnicos de implementação, informação disponível na internet:<URL: https://ec.europa.eu/digital-building-blocks/sites/download/attachments/677512071/eEDES%20-%20Vision%2C%20Governance%2C%20Implementation%2015.11.2023.pdf?version=1&modificationDate=1705392683490&api=v2>. [Consultado em 02/05/2025].

[92] Lei n.º 88/2017, de 21 de agosto, com as alterações introduzidas pela Lei n.º 42/2023, de 10 de agosto, aprova o regime jurídico da emissão, transmissão, reconhecimento e execução de decisões europeias de investigação em matéria penal, transpõe a Diretiva 2014/41/UE, do Parlamento Europeu e do Conselho, de 3 de abril de 2014, e revoga a Lei n.º 25/2009, de 5 de junho, disponível na internet:<URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=2754A0050&nid=2754&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=>. [Consultada em 02/05/2025].

[93] A este respeito a CE disponibiliza informação na internet:<URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en>. [Consultado em 02/05/2025].

transfronteiriças poderem vir a ser notificadas aos Estados visados, prevenindo e antecipando a possibilidade de ocorrência de conflitos de jurisdição.

2.5 Jurisdição em ambiente digital.

Resulta do exposto que compete aos Estados soberanos determinar os limites de alcance das suas leis penais, sendo que, atualmente, a doutrina maioritária aceita que a jurisdição penal nacional se encontra limitada pelo direito internacional, ou seja, pela soberania de Estados terceiros[94].

A questão que agora se coloca é, perante a crescente globalização de interações que ocorrem na internet, dispersão de utilizadores e equipamentos pelas mais diversas jurisdições (desterritorialidade), como é que o direito internacional determina os limites dessas fronteiras digitais?

Podemos inferir dos conceitos e princípios até aqui expostos que é ao Estado a quem compete regular o comportamento penal dos cidadãos dentro dos limites do seu território. Extravasando estes limites, ou seja, regulando o comportamento para lá das suas fronteiras territoriais, estará a interferir em assuntos de um Estado estrangeiro, que é o mesmo que dizer com a soberania deste.

Sem olvidar que o Direito Penal é a *ultima ratio* do poder de intervenção do Estado na vida dos cidadãos, poderia parecer aceitável, que o Estado pudesse regular o comportamento dos cidadãos presentes fisicamente em território nacional, mas também as repercussões que esses comportamentos pudessem vir a ter no território de países terceiros, considerando-os no momento em que tivesse julgar o crime.

Na literatura alemã, questões desta natureza são tratados ao nível da "*legislação penal extraterritorial*", que diga-se, se justifica caso exista um fator de conexão reconhecido pelo Direito Internacional. Destes, podemos referir a título de exemplo, o lugar da prática do crime (que tem subjacente o princípio da territorialidade), a nacionalidade do autor ou da vítima (princípio da personalidade ativa ou passiva), que o crime atente contra bens especialmente importantes do Estado, sobretudo a segurança ou existência (princípio da proteção) e por último que o crime também seja um crime de direito internacional (princípio da universalidade). Devemos, no entanto salientar, que ainda que existam fatores de conexão, a extensão da jurisdição penal nacional a condutas extraterritoriais

[94] (PAYER, 2024, p.209). [Consultado em 08/04/2025].

poderá não ser admissível, caso exista violação da proibição de arbitrariedade ou abuso de direito de acordo com o Direito Internacional.

Aquilo que devemos destacar é que, atualmente, todos os Estados no mundo, reconhecem o princípio da territorialidade. Isto não pode ser dito acerca de nenhum outro princípio de conexão em termos tão absolutos[95]. A projeção deste princípio foi feita a pensar num mundo de fronteiras físicas, no entanto, como temos vindo a tentar demonstrar, com o advento da internet, o acesso transfronteiriço a dados informáticos transfronteiriços causa tensões com a sua aplicação ao ambiente digital "*tendo em conta que o princípio da territorialidade da lei processual penal assenta «na ideia de que a jurisdição penal se contém estritamente dentro dos limites do Estado»*"[96]. Com o aumento da criminalidade informática transnacional, esta clivagem mostra-se ainda mais patente e passível de gerar conflitos jurisdicionais entre países.

A este respeito, recordamos PRADILLO quando refere que *"...la expresión "Internet no conoce fronteras" favorece al delincuente, porque en el plano policial las fronteras nacionales se convierten en auténticos obstáculos para las legítimas labores de investigación y recogida de las evidencias de dichos delitos. Las fuerzas y cuerpos de seguridad deben respetar la soberanía de otros países y, como norma general, no pueden llevar a cabo actividades de investigación y obtención de pruebas fuera de su jurisdicción*"[97].

Veremos, por conseguinte, como é que os diplomas europeus e a nossa legislação abordam a questão das pesquisas informáticas transfronteiriças.

3. AS PESQUISAS INFORMÁTICAS TRANSFRONTEIRIÇAS

3.1 Enquadramento

Não trataremos neste trabalho da Diretiva n.º 2006/24/CE, relativa à conservação de gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva

[95] *Ibidem*, cit., p.210. [Consultado em 08/04/2025].
[96] (RAMALHO, 2017, p. 59) e Minuta do Relatório Explicativo da Convenção Cibercrime, §293, p. 69. Texto integral disponível na internet:<URL:http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf>. [Consultado em 08/04/2025].
[97] 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 na internet:<URL:http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf>. [Consultado em 13/04/2025].

2002/58/CE, nem da Lei n.º 32/2008, de 17 de julho, que a transpôs, essencialmente por dois motivos: não se debruçam sobre dados de conteúdo (cf. Artigo 2.º, n.º 2, alínea a) e 5.º da Diretiva e artigos 2.º, n.º 1, alínea a) e 4.º da Lei n.º 32/2008) e também porque reportam-se a obrigações de conservação de dados informáticos que impendem sobre os fornecedores de serviços de comunicações eletrónicas e não a verdadeiras medidas de recolha de prova digital a serem executadas em sede de investigação criminal, de que nos ocupamos. Assim, não faremos referência à intervenção nas comunicações eletrónicas (v.g. transmissão, comutação ou encaminhamento de sinais por cabo, meios radioelétricos, meios óticos ou por outros meios eletromagnéticos, incluindo as redes de satélites, as redes terrestres fixas incluindo a internet e móveis etc.).

Quando na prática de crimes se utiliza meios informáticos, a busca *online*, por vezes, revela-se o único meio apto para obtenção de informações acerca da autoria. Não podemos esquecer as dificuldades de recolha de prova com que os OPC se deparam.

Perante um cenário desta natureza, constatamos que a legislação portuguesa sobre a cibercriminalidade assenta na transposição de Diretivas, decisões-quadro e outros instrumentos jurídicos de instâncias europeias.

A respeito da recolha de prova digital analisaremos de seguida a Convenção de Budapeste sobre o Cibercrime[98] e no plano nacional, a LCc (Lei n.º 109/2009, de 15 de setembro)[99].

3.2 Convenção sobre o cibercrime - soluções de acesso transfronteiriço a dados informáticos.

A Convenção de Budapeste (CBCc) vigora em Portugal desde o dia 1 de julho de 2010, após depósito do instrumento de ratificação junto do Secretário-Geral do Conselho da Europa, a 24 de março do mesmo ano[100]. Entre ratificações e adesões, a Convenção

[98] A Convenção sobre o Cibercrime foi aprovada e publicada por Resolução da Assembleia da República n.º 88/2009 de 15 de setembro e ratificada pelo Decreto do Presidente da República n.º 92/2009 na mesma data. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://files.dre.pt/1s/2009/09/17900/0635406378.pdf>. [Consultada em 14/04/2025].

[99] A Lei n.º 109/2009 de 15 de setembro que adapta o direito interno à Convenção e à Decisão Quadro n.º 2005/222/JAI. Disponível na internet: <URL:https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis&so_miolo=>. [Consultada em 13/04/2025].

[100] A lista de datas de assinaturas, ratificações/adesões e inícios de vigência encontra-se publicada e disponível na internet: <URL:http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>. [Consultada em 14/04/2025].

conta neste momento com a participação de 78 Estados. Apesar deste número a Convenção tem vindo a servir de referência na harmonização de leis substantivas e leis processuais de vários Estados não-aderentes.

Por sua vez a Organização das Nações Unidas (ONU), em Assembleia Geral adotou as resoluções n.º 55/63[101] e 56/121[102] no âmbito da investigação de crimes contra sistemas de informação sublinhando a importância da necessidade de harmonização, de modo a erradicar *safe havens* (portos seguros) para os criminosos, apelando ainda à troca de informações, cooperação e coordenação entre Estados.

Seguiram-se recomendações de adesão por parte da Organização para a Segurança e Cooperação na Europa (OSCE)[103].

O Comité da Convenção sobre o Cibercrime (doravante T-CY) tem contado com vários Estados Observadores. No plenário de 2018, em que Portugal, representado pelo Ministério Público, foi eleito para a Vice-Presidência do Comité, estiveram presentes Colômbia, Gana, Irlanda, México, Nigéria, Paraguai, Rússia, Tunísia e Singapura como observadores, para além de representantes de várias instituições da União Europeia, da Interpol e do Gabinete das Nações Unidas contra a Drogas e o Crime[104]. De entre os Estados-membros do Conselho da Europa, apenas não ratificaram Irlanda, Suécia e ainda a Rússia que nunca chegou sequer a assinar, manifestando receio pela sua soberania, pela segurança dos Estados-membros e pelos direitos dos seus cidadãos, decorrente das possibilidades de acesso transfronteiriço a dados informáticos no contexto de investigações criminais, inseridas nas disposições do artigo 32.º da Convenção sobre o Cibercrime[105].

Em 2003, a Convenção foi complementada pelo Protocolo Adicional à Convenção sobre o Cibercrime relativo à Criminalização de Atos de Natureza Racista e Xenófoba

---

[101] Texto integral em Inglês da Resolução da Assembleia Geral da Organização das Nações Unidas n.º 55/63, de 4 de dezembro de 2000, disponível na internet:
<URL: https://digitallibrary.un.org/record/428861?ln=en&v=pdf>. [Consultado em 14/04/2025].
[102] Texto integral em Inglês da Resolução da Assembleia Geral da Organização das Nações Unidas n.º 56/121, de 9 de dezembro de 2001, disponível na internet:
<URL: https://digitallibrary.un.org/record/454952?ln=en&v=pdf>. [Consultado em 14/04/2025].
[103] Decisão n.º 7/06 sobre o combate à utilização da Internet para fins terroristas, de 5 de dezembro de 2006, disponível em Inglês na internet:<URL:https://www.osce.org/mc/23078?download=true>. [Consultado em 14/04/2025].
[104] Cf. Ata do 19.º plenário do T-CY, em 9 de julho de 2018, Estrasburgo, disponível na internet:<URL:https://rm.coe.int/tcy-2018-22-plen19rep-v3/16808c376a>. [Consultado em 14/04/2025].
[105] (RAMALHO, 2017, p. 75) e nota 113.

praticados através de Sistemas Informáticos[106]. Tem como objetivo, a complementaridade, pelas Partes das disposições constantes da CBCc e descreve as condutas que as mesmas devem tipificar, nos respetivos direitos internos, como infrações penais relativamente à difusão, ou outras formas de colocação à disposição do público, através de um sistema informático, de material racista e xenófobo.

A CBCc teve, essencialmente, três objetivos[107] e visou principalmente: i) a harmonização dos elementos de direito penal substantivo interno das infrações e as disposições conexas no domínio do cibercrime, ii) a definição, ao abrigo do processo penal nacional, dos poderes necessários para a investigação e a repressão de tais infrações, assim como de outras infrações cometidas por meio de um sistema informático ou relacionadas com a utilização de provas sob a forma eletrónica de outros crimes, e iii) a criação de um regime rápido e eficaz de cooperação internacional[108].

O consenso então obtido entre as Partes para adaptação do direito interno à Convenção teve como contrapartida a assunção de que a mesma não tornaria possível, por si só, qualquer intrusão na soberania nacional das Partes para a perseguição criminal de quaisquer ilícitos, salvo mecanismo jurídico de cariz supranacional que dispusesse em sentido contrário[109]. Assim, é a legislação nacional dos Estados e para o que importa neste estudo, a portuguesa, que regula os meios processuais de recolha da prova digital. Desta forma a Convenção, salvo acordo internacional ou caso se encontrem preenchidos os requisitos do artigo 32.º da Convenção, privilegia o recurso à cooperação internacional na recolha de prova digital armazenada em sistemas informáticos que se encontrem situados noutro ordenamento jurídico. Foi tendo presente situações como podermos ser confrontados com uma investigação nacional em que as autoridades descobrem que o suspeito armazenou dados informáticos de valor probatório num sistema informático localizado noutro Estado, ao qual se poder aceder remotamente em território nacional com recurso a qualquer sistema informático ligado à internet (*v.g* um fornecedor de

[106] Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802ed8cd>. [Consultada em 14/04/2025].
[107] RAMALHO, David Silva, *A recolha de prova penal em sistemas de computação em nuvem* in *Revista de Direito Intelectual*, n.º 2 (Dez. 2014), pp. 123-162, p.133, disponível na internet:<URL: https://catalogo.pgr.pt/cgi-bin/koha/opac-detail.pl?biblionumber=246778>. [Consultado em 14/04/2025]
[108] Relatório Explicativo ao Segundo Protocolo Adicional à Convenção sobre o Cibercrime, §6, p.2. disponível na internet: <URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680aa2b7c>. [Consultado em 16/04/2025].
[109] (RAMALHO, 2014, p.133). [Consultado em 14/04/2025].

serviços de *webmail*), que o Relatório Explicativo da Convenção esclareceu que o procedimento de busca e apreensão de dados informáticos armazenados, previsto no artigo 19.º da CBCc, não «*confere aos Estados a possibilidade de busca e apreensão de dados no seio do território de outras Partes, sem que seja necessário recorrer às modalidades tradicionais de assistência jurídica mútua*»[110]. Para esse desiderato, o artigo 32.º da CBCc, como veremos, elenca as situações excecionais em que é admissível o acesso transfronteiriço (unilateral) a dados informáticos armazenados em sistemas informáticos que se encontrem no estrangeiro, sem necessidade de autorização ou notificação do Estado visado. A este respeito os redatores da Convenção, após longos debates, chegaram à conclusão de que, naquela fase, não seria ainda possível elaborar um regime global, legalmente vinculatório, que regulamentasse esta matéria, essencialmente por dois motivos: o primeiro a ausência de uma experiência objetiva relativamente a este tipo de situações e a segunda por considerarem que a resolução adequada está, frequentemente, ligada à conjuntura do caso em concreto, pelo que se tona difícil estipular regras gerais. Decidiram que apenas seriam definidas, ao abrigo do Artigo 32.º da Convenção, as situações nas quais, por unanimidade, a ação unilateral se mostrasse aceitável[111]. Seguiu, no essencial, os princípios delineados pela Conferência Ministerial dos países do G8 sobre o Combate à Criminalidade Organizada Transnacional, que teve lugar a 19 e 20 de outubro de 1999, em Moscovo[112].

A este respeito e em sede própria veremos como esta intenção veiculada na Convenção e aquela que resulta da LCc poderá dar azo a interpretações que podem contrariar o espírito de cooperação que presidiu à primeira.

3.2.1 Acesso transfronteiriço a dados informáticos armazenados publicamente acessíveis.

Este acesso encontra-se previsto e regulado no artigo 32.º, alínea a) da CBCc e prevê o acesso a dados informáticos armazenados pública e livremente acessíveis, independentemente da sua localização geográfica, sem que para isso haja necessidade de

[110] Minuta do Relatório Explicativo, §195, p. 44, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802fa429>. [Consultado em 14/04/2025].
[111] *Ibidem*, §293, p. 69.
[112] Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf>. [Consultado em 14/04/2025].

acionar mecanismos de cooperação internacional. Compreendidos nesta categoria encontram-se todos os dados cuja acessibilidade não dependa de especiais pré-requisitos. Não constitui sequer obstáculo, por si só, que os dados se encontrem sujeitos a alguma forma de controlo de acesso, como a necessidade de pagamento, subscrição ou registo, desde que esses serviços se encontrem disponíveis ao público, como acontece, por exemplo, com as redes sociais[113].

Relembramos que o Relatório Justificativo da Convenção sobre o Cibercrime se referia a dados desta natureza na parte em que os redatores referiram as situações, nas quais, por unanimidade, a ação unilateral se mostrava aceitável (ao abrigo do artigo 32.º da Convenção), em termos que "*Assim, os redactores da Convenção acabaram por consagrar na alínea a) do art.º 32 do texto final uma permissão genérica de recolha de prova armazenada em servidores estrangeiros quando os dados a recolher se encontrem publicamente acessíveis*"[114].

Ainda assim, entendemos relevante salientar e destacar a posição de BERT-JAAP KOOPS no sentido de naquelas situações de disponibilidade de dados informáticos em fonte aberta (livremente acessíveis e muitas vezes utilizados pelos OPC para recolha de informação que se revela útil nas investigações em curso), no seguimento da jurisprudência do Tribunal Europeu dos Direitos Humanos, mesmo em público existe uma expetativa legítima de privacidade[115], que, aplicada analogicamente à atuação dos indivíduos na *World Wide Web*, resulta na sua crença de que aquilo que publicam *online* não será efetivamente acedido por toda a gente, órgãos de polícia incluídos. Se pesquisas isoladas com recurso a motores de busca convencionais não apresentam ameaça de maior à privacidade dos sujeitos objeto das pesquisas, o mesmo não se poderá dizer quando estes sejam alvo de pesquisas sistemáticas, especialmente quando feitas com recurso a instrumentos de recolha e/ou tratamento automatizado de dados[116].

---

[113] Cf. (RAMALHO, 2017, pp. 72-73); ainda COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, T-CY Guidance Note # 3 – Transborder access to data (Article 32), 2014 (a), p. 4, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transbprder-access-to-data.pdf >.

[114] (RAMALHO, 2014, p. 135).

[115] Koops, Bert-Jaap, *Police investigations in Internet open sources: Procedural-law issues, 29 Computer Law & Security Review (6)*, 2013, (pp. 654-665), disponível na internet:<URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2574951>. [Consultado em 14/04/2025].

[116] Cf. Acórdão da Quarta Secção do TEDH de 12 de janeiro de 2010, Guillan e Quinton c. Reino Unido, queixa n.º 4158/05 e acórdão da Terceira Secção do TEDH de 24 de junho de 2004, Von Hannover c. Alemanha, queixa n.º 59320/00, disponíveis, respetivamente, na internet:<URL:https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-96585%22]}> e

Em 2003, a Convenção foi complementada pelo Protocolo Adicional à Convenção sobre o Cibercrime relativo à Criminalização de Atos de Natureza Racista e Xenófoba praticados através de Sistemas Informáticos (STCE n.º 189, a seguir designado por "Primeiro Protocolo")[117].

3.2.2 Acesso transfronteiriço a dados informáticos armazenados mediante consentimento da pessoa legalmente autorizada.

Dispõe o artigo 32.º, alínea b), da Convenção sobre o Cibercrime que *"[u]ma Parte pode, sem autorização de uma outra Parte […] [a]través de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através desse sistema informático*"[118]. Refere ainda DAVID RAMALHO que surgem problemas com a densificação do conceito de pessoa com legitimidade para divulgar os dados[119], cujo significado poderá variar em função da legislação de cada Estado-signatário, transcrevendo o esclarecimento do Relatório Justificativo da Convenção sobre o Cibercrime, no parágrafo 294[120]. Pode, em suma, variar em função da legislação interna de cada um dos Estados-Signatários, da forma como o conceito é configurado e da forma como é aferida a legalidade do consentimento prestado. Fulcral, nas suas palavras é que a legislação do Estado requisitante configure tal consentimento como válido e que o mesmo seja voluntário, livre e informado[121]. Devemos ter presente que este consentimento não deve surgir no seguimento de manobras ardilosas (*v.g.* utilização de *Keyloggers*) ou medidas coercivas (*v.g.* a injunção para apresentação ou concessão de acesso a dados). Só assim de consegue assegurar e aferir a voluntariedade do consentimento.

A maior parte das vezes, a pessoa com legitimidade para a divulgação de dados será o próprio titular que poderá ter correspondência com um arguido ou ofendido em

<URL:https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-61853%22]}>. [Consultado em 14/04/2025].

[117] Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802ed8cd>. [Consultado em 14/04/2025].

[118] (RAMALHO, 2014, p.137) e (RAMALHO, 2017, pp. 73-74).

[119] *Ibidem*, cit. respetivamente, p.137 e p. 74.

[120] Minuta do Relatório Explicativo, §294, p. 70, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802fa429>. [Consultado em 14/04/2025].

[121] (RAMALHO, 2014, p.137) e (RAMALHO, 2017, p. 74).

processo-crime. No entanto, por vezes, podemos estar perante um terceiro que se apresente com legitimidade para consentir o acesso aos dados, nomeadamente quando sejam utilizados meios por si titulados (*v.g.* equipamentos de um empregador) ou *Internet Service Providers* (ISP) nos quais se incluem as operadoras de internet, os serviços de *webmail* ou de armazenamento em *cloud*[122]. De acordo com o critério avançado por NICOLAI SEITZ, estes ISP estarão apenas legitimados a divulgar os dados se, for sua a vontade de o armazenamento ser efetuado em servidores localizados no território de outro Estado (aos quais possam de facto aceder) e não da vontade do titular[123].

Apesar da referência ao lugar onde a pessoa que presta o consentimento ser omissa na Convenção, a maior dos Estados- Signatários rejeitam uma abordagem direta por parte de Estados terceiros a cidadãos que se encontrem nos seus territórios, com vista a obter a sua colaboração[124].

Já o Regulamento Geral de Proteção de Dados (RGPD)[125] prevê no artigo 7.º, n.º 3, que a revogação do consentimento para tratamento de dados pessoais não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.

Em suma, o artigo 32.º, alínea b) da Convenção sobre o Cibercrime cobre todas aquelas situações de colaboração voluntária com as autoridades que dirigem uma investigação, repetimos, sem manobras ardilosas ou medidas coercivas. No entanto, existem autores que, mesmo na ausência de coercividade, entendem que os atos praticados ao abrigo desta alínea continuam a ser suscetíveis de atentar contra a soberania do Estado visado, caso não seja seu o consentimento prestado[126]. Os defensores desta perda de soberania apresentam o argumento que a soberania nacional não é disponível a um particular ou pessoa coletiva, pelo menos sem que se mostrem definidos

---

[122] *Ibidem*.
[123] SEITZ, Nicolai, *Transborder Search: A New Perspective in Law Enforcement, 7 Yale J.L. & Tech.23*, 2005, (pp. 45-45), disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://yjolt.org/sites/default/files/seitz-7-yjolt-23.pdf >. [Consultado em 14/04/2025]; Minuta do Relatório Explicativo, §294, p. 70.
[124] Cf. COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *Transborder access and jurisdiction: What are the options?*, 2012, p. 23, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802e79e8>.
[125] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível na internet: <URL:https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis>. [Consultado em 14/04/2025].
[126] Neste sentido GERCKE, Marco, *Understanding Cybercrime: phenomena, challenges and legal response*, 2012, pp. 277-278, disponível na internet: <URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.itu.int/ITU-D/cyb/Cybersecurity/docs/cybercrime%20legislation%20EV6.pdf >. [Consultado em 14/04/2025]; de igual forma a doutrina alemã, SEITZ, Nicolai, cit., p. 40.

procedimentos concretos para o efeito, algo que, referem, a Convenção não faz. Inclusive, este é um dos principais motivos, como já referimos, para a oposição da Federação Russa à Convenção, membro do Conselho da Europa, que tem recusado a assinatura da Convenção, porquanto, no seu entendimento, o artigo 32.º, al. b) "*poderia danificar a soberania e a segurança dos Estados membros e os direitos dos seus cidadãos*"[127].

Estas são as duas exceções ao princípio da territorialidade previstas na CBCc, mas desde já se nos coloca a situação que pode ocorrer, se o acesso decorrer sem o consentimento da pessoa legalmente autorizada a divulga-los. Nesta situação, não se mostrando verificados os requisitos de exceção, o acesso e recolha de prova remota que se justifique terá, forçosamente, que ocorrer através dos mecanismos de cooperação internacional.

3.3 A Lei do Cibercrime - acesso transfronteiriço a dados informáticos armazenados.

Na redação do artigo 19.º, n.º 1 e n.º 2 da CBCc (Busca e apreensão de dados informáticos armazenados), os relatores clarificaram que a opção de fazer constar a menção "*no seu território*", servia para realçar o facto de que a disposição desse artigo, bem como os demais da Convenção, se aplicavam a medidas a serem empreendidas a nível nacional. Clarificaram isso mesmo no Relatório Justificativo da Convenção sobre o Cibercrime[128].

Acontece que, na adaptação da lei portuguesa ao artigo 19.º da Convenção, o legislador suprimiu na LCc[129], qualquer referência à limitação territorial das pesquisas informáticas a realizar por via remota a um sistema informático acessível através daquele que é objeto da pesquisa. O artigo 15.º, n.º 5 dispõe[130]: "*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*".

---

[127] Cf. (RAMALHO, 2017, p. 75) e nota 113.
[128] Minuta do Relatório Explicativo, §192 e 193, p. 43, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/16802fa429>. [Consultado em 14/04/2025].
[129] LCc disponível na internet:<URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis&so_miolo=>. [Consultada em 15/04/2025].
[130] Pesquisa de dados informáticos que em termos processuais, com as necessárias adaptações, configura uma verdadeira busca por força do n.º 6.

A redação desta disposição suscitou controvérsia relativamente à forma como deveria ser interpretada. Uma, restritiva, apontava no sentido de apesar da expressão "*no seu território*" ter sido suprimida, a norma deveria, ainda assim, ser lida e interpretada de acordo com a fonte, ou seja, a Convenção sobre o Cibercrime. Neste sentido, ainda que de forma implícita, a delimitação territorial constava, "…*pelo que a pesquisa informática a que se refere o n.º 5 do artigo 15.º da Lei do Cibercrime é aplicável somente em território português, isto é limitada aos casos em que os dados informáticos visados se encontram armazenados num sistema informático fisicamente localizado em território português, independentemente de ser, ou não, possível aceder a esse sistema a partir de outro sistema informático também localizado em Portugal*.

Uma outra interpretação, perfilhada por DAVID RAMALHO, de cariz fundamentalmente literal e teleológico, vai no sentido de que "*a pesquisa informática e, consequentemente, a apreensão de dados informáticos, por parte de autoridades portuguesas, a sistemas informáticos acessíveis através de outro sistema localizado em território português não encontra qualquer limitação territorial, sendo genericamente admitida, desde que, naturalmente, o acesso ao outro sistema informático seja lícito*"[131]. Em nota de rodapé, refere o autor que esta posição traduz a que é sustentada por PEDRO VERDELHO.

Fundamenta a sua posição, concluindo que a ausência de delimitação territorial na LCc, apesar de contrária ao texto que lhe serviu de fonte (a Convenção) foi intencional. Por outras palavras, na transposição para o direito interno, quis o legislador no artigo 15.º, n.º 5 da LCc, ampliar o âmbito de aplicação do artigo 19.º da Convenção, tornando lícita, no plano interno, uma recolha de prova que, na perspetiva do Estado no qual se encontrem os dados, poderá ser ilícita. Seria esta a interpretação que nas suas palavras "*Em face da omissão – presumivelmente intencional, porquanto contrária ao texto que lhe serviu de fonte – da referência a qualquer limitação territorial na aplicação destas medidas, é esta a interpretação que se nos afigura mais correcta, por ser a mais consentânea com o espírito e a letra da lei*"[132]. Ainda de acordo com o autor, subjacente a esta opção legislativa estariam em confronto duas teses: "*de um lado, a da configuração do acesso a sistemas informáticos localizados no estrangeiro como um acto processual com natureza e implicações puramente nacionais; de outro lado, o reconhecimento da bondade das premissas sobre as quais assentou a Convenção, relativas à necessidade de*

[131] (RAMALHO, 2014, p. 141).
[132] *Ibidem*, cit., p. 142.

acordo entre os Estados para o acesso transfronteiriço a dados informáticos, e subsequente opção pela sua desconsideração em prol da eficácia penal"[133]. Em termos sucintos, em defesa da primeira o argumento seria que "*o acesso remoto a um sistema de computação em nuvem, ao ser efectuado a partir de um sistema informático localizado em território nacional, se encontra abrangido pela lei processual penal portuguesa, porquanto o acesso aos dados é feito a partir de território português. Assim, a pesquisa e subsequente apreensão dos dados informáticos visados em nada interfere com a soberania do(s) Estado(s) no(s) qual(is) se encontra a nuvem*"[134]. Neste plano, argumenta que dificilmente se poderá sustentar este entendimento da medida em que o acesso traduz-se na ativação de funcionalidades de processamento informático em *hardware* localizados no espaço físico do Estado terceiro, motivo pelo qual o acesso não será assim desprovido de materialidade nesse Estado. Existindo transferência de prova armazenada no sistema desse Estado terceiro para o território português, verificava-se uma aplicação de medidas de natureza processual penal, enquanto exercício do poder estatal, com objeto e repercussões no Estado terceiro soberano, sem que as autoridades desse Estado tivessem conhecimento de tais atos.

Este entendimento - que refuta ter sido o que sustentou a opção legislativa - considera que não só contraria os pressupostos do texto original da Convenção mas também conflitua com o disposto no artigo 25.º da LCc, que prevê os casos em que as autoridades estrangeiras, poderão proceder ao acesso *transfronteiriço* de dados informáticos armazenados em território português. Nesse sentido, apontou que se o legislador português consciente dessa materialidade (repercussões em território nacional) pressupôs a necessidade de autorização para que as autoridades estrangeiras possam aceder a dados informáticos armazenados em território português, não poderia sustentar-se o contrário em conduta inversa, por parte das autoridades portuguesas[135], ou seja, que sendo o acesso efetuado por parte das autoridades portuguesas, essa ação não teria implicações no Estado visado pela pesquisa.

Segundo o autor, "*Admitindo-se, então, que o legislador português reconhece que o acesso transfronteiriço a dados informáticos traduz na prática de actos processuais com efeito noutra jurisdição, e que, ainda assim, consagrou a admissibilidade de aplicação da lei processual penal portuguesa aos mesmos actos, em desconformidade com o*

[133] *Ibidem.*
[134] *Ibidem*.
[135] *Ibidem*, cit., p.143.

princípio da territorialidade tal como se encontra configurado no artigo 6.º do Código de Processo Penal (CPP), sem dispositivo de cariz supranacional que o legitime, resta concluir que o fez sem ignorar a potencial ilicitude desse acesso no plano interno do Estado-destinatário da pesquisa e apreensão.

Assim, confrontado com um bloqueio de ordem jurisdicional ao exercício da acção penal, o legislador português optou por remover unilateralmente os obstáculos à eficácia da investigação criminal, indo mais longe do que os termos previstos na Convenção"[136].

Esta opção legislativa (seguida noutros Estados signatários da Convenção) é criticável para alguns opositores que questionam as consequências práticas da extensão da aplicabilidade espacial da lei processual penal a sistemas informáticos localizados noutros Estados, enfatizando os riscos decorrentes da sua subtração à regra da territorialidade. Assinalam os riscos de existência de investigações simultâneas paralelas em diferentes Estados, com os riscos associado de contaminação e/ou eliminação da prova digital.

Por outro lado, também no plano da sua coerência interna, a LCc[137] não escapou à crítica doutrinária, num primeiro momento devido à opção do legislador por mais uma lei extravagante em detrimento de uma revisão do regime geral. A dispersão legislativa do processo penal a isso desaconselhava.

Nesta lei, de transposição para o ordenamento interno da Convenção sobre o Cibercrime (adaptando o artigo 14.º, n.º 2, alíneas b) e c)), o legislador criou regras processuais de natureza geral, não só aplicáveis à cibercriminalidade (artigo 11.º, n.º 1, alínea a) da Lei), mas também o todo o tipo de crimes cometidos por meio de um sistema informático (artigo 11.º, n.º 1. alíneas b) e c) da Lei).

Em matéria de acesso transfronteiriço por autoridades estrangeiras competentes a dados informáticos armazenados em Portugal, o legislador foi ao encontro das soluções da Convenção: permissão de acesso a dados de fonte aberta ou mediante o consentimento da pessoa legalmente autorizada (artigo 25.º da LCc).

Ora, um dos problemas que se colocava era a conjugação do disposto no artigo 15.º, n.º 5 com as normas do artigo 25.º do mesmo diploma, que consagram na legislação portuguesa as disposições previstas no artigo 32.º da Convenção sobre o Cibercrime[138].

---

[136] *Ibidem*.

[137] A Lei n.º 109/2009, de 15 de setembro, que aprovou a Lei do Cibercrime, veio cumprir os compromissos internacionais decorrentes da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e da Convenção sobre o Cibercrime, do Conselho da Europa. Tendo entrado em vigor a 15 de outubro de 2009, revogou, então, a sua antecessora, a Lei da Criminalidade Informática, Lei n.º 109/91, de 17 de agosto.

[138] (RAMALHO, 2014, p. 145).

O artigo 25.º da LCc prevê, nas duas alíneas, sem necessidade de pedido prévio às autoridades portuguesas, o livre acesso a dados armazenados em território português em duas situações: quando esses dados são publicamente disponíveis e; mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulga-los. Não se mostrando verificados estes requisitos, as autoridades estrangeiras terão de recorrer aos mecanismos de cooperação internacional, quando pretendam recolher, remotamente, prova armazenada em território português. Conjugando este artigo 25.º com o disposto no artigo 15.º, n.º 5, ambos da LCc, onde o legislador nacional ampliou o âmbito de aplicação das pesquisas informáticas a dados armazenados, possibilitando nas investigações criminais nacionais a realização de acessos transfronteiriços, retiramos a existência de uma competência irrestrita às autoridades nacionais no que respeita à pesquisa e apreensão remota de dados armazenado em território estrangeiro, no entanto, em condições de reciprocidade de investigações veda esse acesso às autoridades estrangeiras quando estas pretendam recolher prova em sistemas que se encontrem em território português, salvo se se verificar uma das exceções previstas no artigo 25.º da LCc.

3.4 Lei do Cibercrime - pesquisa e apreensão de dados.

O CCP consagra os regimes jurídicos das buscas e apreensões, como meios de obtenção de prova nos artigos 174º a 186º. Na LCc, os artigos 15.º a 17.º consagram um regime paralelo de buscas informáticas (legalmente referidas como pesquisas) e de apreensão de dados, visando adaptar às exigências do mundo digital aqueles meios de aquisição de prova.

O artigo 15º da LCc permite que a autoridade judiciária (AJ) competente autorize uma pesquisa a um sistema informático quando, no decurso de uma investigação, tal se revele necessário para a aquisição e recolha de prova. Por sua vez, o artigo 16º dispõe relativamente ao processo de apreensão dos dados informáticos que, no decurso de uma pesquisa (ou outro acesso legítimo a um sistema), se mostrem necessários à produção de prova e descoberta da verdade.

Relativamente à pesquisa de dados informáticos, o artigo 15.º, n.º 3, regula os casos em que os OPC podem proceder à pesquisa sem prévia autorização da AJ, dispondo a alínea a), quando "*a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados*". Não será, de igual forma, exigível a intervenção da AJ, quando nos termos do artigo 16.º, n.º 1 e n.º 2 da LCc "*quando haja urgência ou perigo na demora".*

Contudo, é legalmente exigível a intervenção do juiz de instrução criminal (JIC) quando se revela necessário proceder à apreensão de alguns tipos de dados, nomeadamente, quando nos termos do artigo 16.º, n.º 3 sejam apreendidos "*dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro*", ou nos termos do artigo 17.º, se estivermos perante uma apreensão de correio eletrónico ou de registos de comunicações de natureza semelhante. Por conseguinte, se no âmbito de uma investigação ocorrer uma das situações de apreensão coerciva de dados mencionadas, como salvaguarda dos direitos fundamentais à privacidade, intimidade e sigilo de comunicações, suscita-se não só a intervenção do Ministério Público (MP), como também se mostra exigível a intervenção judicial.

Todavia, perante situações que não careçam da intervenção judicial e em que não se mostra necessário o recurso aos diversos mecanismos coercivos dos artigos 15º, 16º e 17º da LCc, os OPC podem apreender para o processo todos os dados que se mostrem úteis e relevantes em termos probatórios para a investigação.

Devemos realçar que o consentimento prestado deverá traduzir-se numa declaração expressa, preferencialmente, documentada. O artigo 15º, nº 3, alínea a) da LCc exige que o consentimento "*fique, por alguma forma, documentado*". Será desejável que o seu teor seja claro, esclarecido e inequívoco. Neste sentido, quando o titular dos dados consente, autoriza o acesso aos dados informáticos e a sua apreensão, não é exigível qualquer autorização da AJ, quer para o acesso aos dados (pesquisa), quer para a apreensão e conhecimento dos mesmos.

Neste sentido, nas palavras de PEDRO VERDELHO "*Esta conclusão é também válida para dados em relação aos quais, nos casos de apreensão coerciva (portanto sem consentimento), se requere intervenção judicial. É o caso dos chamados dados pessoais ou íntimos (artigo 16º, nº 3 da Lei do Cibercrime) e do correio eletrónico ou registos de natureza semelhante (artigo 17º). Quando se torna necessário apreender dados destas naturezas e não há consentimento de acesso aos dados em causa, é exigida intervenção judicial; porém, caso seja prestado consentimento e o mesmo documentado, não se torna a necessária intervenção judicial. A intervenção judicial é uma garantia processual adicional que a lei confere aos cidadãos. Porém, não estando em causa direitos*

indisponíveis, podem esses mesmos cidadãos prescindir na mesma, consentindo o acesso aos dados[139].

3.5 Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da Cooperação e da Comunicação de Provas Eletrónicas.

Já referimos como as tecnologias da informação e da comunicação (TIC) evoluíram e transformaram as sociedades a nível mundial.

Mesmo depois da entrada em vigor da CBCc, registou-se um aumento significativo da exploração da tecnologia para fins criminosos. Os exemplos incluem a violência sexual *online* contra crianças e outros crimes contra a dignidade e a integridade das pessoas, roubo e uso abusivo de dados pessoais entre outros. Em 2020 e 2021, durante a pandemia de Covid-19, observou-se ainda um aumento significativo do cibercrime, incluindo ataques a hospitais e instalações médicas que desenvolviam vacinas contra o vírus, uso abusivo de nomes de domínio para promover vacinas, tratamentos e curas falsas, e outros tipos de atividades fraudulentas.

Apesar deste crescimento, os conceitos consagrados na CBCc são tecnologicamente neutros, de modo a que o direito penal substantivo possa ser aplicado tanto às tecnologias atuais como às futuras tecnologias envolvidas. Já aqui aludimos[140] aos objetivos da CBCc[141].

As Partes signatárias da CBCc têm, ao longo dos anos da sua vigência, procurado combater o cibercrime recorrendo a vários mecanismos e organismos criados ao abrigo da Convenção, adotando as medidas necessárias para permitir investigações e processos penais mais eficazes. De forma determinante, a utilização e a aplicação da Convenção são facilitadas pelo Comité da Convenção sobre o Cibercrime (T-CY), criado ao abrigo do artigo 46.º da Convenção.

Em 2012, o T-CY, em linha com o seu mandato nos termos do artigo 46.º, n.º 1, da Convenção, de partilhar "informação sobre os desenvolvimentos jurídicos, políticos ou

---

[139] VERDELHO, Pedro, *Pesquisa e Apreensão de dados com consentimento do titular, Nota Prática nº 29/2025 21 de abril de 2025*. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cibercrime.ministeriopublico.pt/sites/default/files/2025-04/nota-pratica-pesquisa-e-apreensao-de-dados-consentidas-2025.04.21.pdf>. [Consultado em 22/04/2025].

[140] Cf. Supra p. 61 (nt. 107).

[141] Relatório Explicativo ao Segundo Protocolo Adicional à Convenção sobre o Cibercrime, §6, p.2. disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680aa2b7c>. [Consultado em 16/04/2025].

técnicos importantes verificados no domínio do cibercrime e a recolha de provas sob forma eletrónica" e para ponderar a possibilidade de "complementar ou aditar a Convenção", criou o subgrupo *ad hoc* sobre a jurisdição e o acesso transfronteiras a dados ("*Transborder Group*"). Em dezembro de 2014, o T-CY concluiu igualmente uma avaliação das disposições em matéria de assistência mútua da Convenção sobre o Cibercrime e adotou um conjunto de recomendações, incluindo algumas que deviam ser abordadas num novo protocolo à Convenção. Estes esforços conduziram à criação, em 2015, do grupo de trabalho sobre o acesso da justiça penal aos elementos de prova armazenados na *cloud*, nomeadamente através da assistência jurídica mútua ("*Cloud Evidence Group*")[142].

Em 2016, o *Cloud Evidence Group* concluiu, entre outros, que "o cibercrime, o número de dispositivos, serviços e utilizadores (incluindo de dispositivos e serviços móveis) e, consequentemente, o número de vítimas atingiu proporções tais que apenas uma pequena parte do cibercrime ou de outras infrações que envolvam provas sob a forma eletrónica será alguma vez registada e investigada. A grande maioria das vítimas de cibercrime não pode esperar que seja feita justiça. Os principais desafios identificados pelo grupo estavam relacionados com a "computação na *cloud*, a territorialidade e a jurisdição" e, por conseguinte, com as dificuldades em obter um acesso eficiente a provas sob a forma eletrónica ou a sua divulgação[143].

Ao avaliar as conclusões do *Cloud Evidence Group*, as Partes na Convenção concluíram que não era necessário aditar ou prever uma criminalização adicional através de disposições de direito penal substantivo. As Partes determinaram, contudo, que eram necessárias medidas adicionais para melhorar a cooperação e a capacidade de as autoridades de justiça penal obterem provas sob a forma eletrónica através de um segundo protocolo adicional, a fim de permitir uma resposta mais eficaz da justiça penal e defender o Estado de direito[144].

A 17.ª reunião plenária do T-CY (8 de junho de 2017) aprovou o mandato para a preparação do presente Protocolo com base numa proposta elaborada pelo *Cloud Evidence Group* do T-CY. Decidiu iniciar a redação do presente Protocolo por sua própria iniciativa, nos termos do artigo 46.º, n.º 1, alínea c), da Convenção. Em 14 de junho de

[142] *Ibidem*, §9, p.3.
[143] *Ibidem*, §10, p.3.
[144] *Ibidem*, §11, p.3.

2017, o Secretário-Geral Adjunto do Conselho da Europa informou o Comité de Ministros (1289.ª Reunião dos Delegados dos Ministros) desta iniciativa do T-CY[145].

A 24.ª sessão plenária do T-CY, em 28 de maio de 2021, aprovou este projeto de Protocolo e decidiu apresentá-lo ao Comité de Ministros, tendo em vista a sua adoção[146].

Em termos de conteúdo, o ponto de partida para o trabalho sobre este Protocolo foi o resultado da avaliação do T-CY das disposições da Convenção relativas à assistência mútua em 2014 e as análises e recomendações do *Transborder Group* e do *Cloud Evidence Group* do T-CY em 2014 e 2017, respetivamente. Os desafios que suscitaram uma preocupação particular referem-se à territorialidade e à jurisdição relacionadas com as provas sob a forma eletrónica, ou seja, que os dados especificados necessários para uma investigação criminal podem ser armazenados em jurisdições múltiplas, móveis ou desconhecidas ("na *cloud*") e a necessidade de soluções para obter a divulgação desses dados de forma eficaz e eficiente para efeitos de investigações ou processos penais específicos[147].

Recordamos, por se revelar de interesse para o tema que abordamos, que dos trabalhos realizados pelo *Transborder Group* resultou, o já mencionado, relatório "*Transborder access and jurisdiction: What are the options?*".

A Decisão (EU) 2023/436 do Conselho de 14 de fevereiro de 2023 autorizou os Estados-Membros a ratificar, no interesse da União Europeia, o Segundo Protocolo Adicional à Convenção sobre o Cibercrime, relativo ao reforço da cooperação e da comunicação de provas eletrónicas[148].

Assim, tendo em conta a complexidade destes desafios, podemos referir, em termos sucintos que neste Segundo Protocolo foram desenvolvidos esforços em específico, nomeadamente de cooperação direta com os prestadores de serviços (artigos 6.º e 7.º), reforço a cooperação para a comunicação de dados informáticos armazenados, (artigos 8.º e 9.º), estabelecimento de procedimentos relativos ao auxílio mútuo de emergência, aplicáveis (artigo 10.º) e estabelecimento de procedimentos relativos à cooperação internacional na ausência de acordos internacionais aplicáveis (artigos 11.º e 12.º).

---

[145] *Ibidem*, §12, p.4.
[146] *Ibidem*, §21, p.4.
[147] *Ibidem*, §22, p.5.
[148] Publicado no JO L 63 de 28.2.2023, p. 48-53. Disponível na internet:<URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023D0436>. [Consultado em 16/04/2025].

Os redatores analisaram igualmente outras medidas que, após uma discussão aprofundada, não foram incluídas no Protocolo. Duas destas disposições, a saber, **"investigações infiltradas ou por meio de sistema informático"** e **"extensão das buscas"**, eram de grande interesse para as Partes, mas foram consideradas como necessitando de trabalho, tempo e consultas adicionais com os intervenientes, pelo que não foram consideradas viáveis no prazo estabelecido para a preparação do presente Protocolo. Os redatores propuseram que estas medidas fossem prosseguidas num formato diferente e, eventualmente, num instrumento jurídico distinto[149].

Recentremos agora o foco no segundo tema que nos propusemos analisar, por sinal um dos afastados deste Segundo Protocolo. Na verdade, perante as inúmeras dificuldades de recolha de prova digital, por vezes mostra-se útil, senão mesmo imprescindível, o recurso a métodos de investigação ocultos em ambiente digital.

4. AÇÕES ENCOBERTAS EM AMBIENTE DIGITAL

A figura do agente encoberto (AE) é em muitas investigações criminais uma ferramenta essencial na obtenção de prova e meio de descoberta da verdade material.

A sua utilização, por colidir com Direitos, Liberdades e Garantias dos cidadãos, leva a que nas sociedades democráticas o sem emprego ocorra e situações muito específicas.

A sua importância foi reconhecida pela Organização das Nações Unidas (ONU) na Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional[150].

Se a figura e modo de atuação do AE já se revela envolta em particularidades, requisitos e especificidades próprias no plano de uma intervenção física, quando nos deparamos com a prática de crimes com recurso a meios tecnológicos e cuja recolha de prova incida, primordialmente, em prova digital, a sua utilização (no ciberespaço) e enquadramento legal suscita dúvidas e vicissitudes acrescidas.

Abordaremos, neste capítulo, o regime do AE e a sua aplicabilidade às investigações realizadas através de meios informáticos levando em conta muito do que foi exposto relativamente a investigações com pontos de contato em vários países (desterritorialidade)

---

[149] Relatório Explicativo ao Segundo Protocolo…, cit., §24, p.6. disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680aa2b7c>. [Consultado em 16/04/2025].

[150] Cf. artigo 20.º, n.º 1 da Convenção, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dcjri.ministeriopublico.pt//sites/default/files/documentos/instrumentos/convencao_nu_criminalidade_organizada_transnacional.pdf>. [Consultada em 29/04/2025].

que levou DANIEL FREIRE E ALMEIDA[151] a defender a criação de um Tribunal Internacional para a Internet para dirimir conflitos cíveis e comerciais, advogando que *"[o] sistema no qual funciona a internet é indiferente quanto à localização física dos computadores, e não há ligação necessária e precisa entre um endereço de Internet e uma jurisdição física*".

Este capítulo tem como propósito analisar não só esta figura como também a sua intervenção em investigações em ambiente digital, nomeadamente, através do recurso a *software* oculto de extração de informação de sistemas informáticos utilizados pelos cibercriminosos, o *malware* que desenvolveremos no último capítulo desta dissertação.

4.1 As medidas antiforenses ou contraforenses.

Devido ao sucesso de investigações como a do *Silk Road*[152], a evolução da Ciência Forense Digital e a crescente intromissão estatal no conteúdo das telecomunicações, tem sido desenvolvidos 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[153].

Nesta fase, é compreensível que uma das maiores justificações para a utilização deste meio intrusivo de recolha de prova (ações encobertas digitais), está diretamente relacionado com a maior sofisticação dos meios tecnológicos utilizados pelos cibercriminosos (organizações) e ao crescente recurso a medidas antiforenses.

Numa definição conceptual, podemos relembrar RYAN HARRIS, quando referia que 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*"[154].

---

[151] *Apud* RAMOS, Armando Dias, *O Agente Encoberto Digital, Meios Especiais e Técnicos de Investigação Criminal*. Coimbra: Almedina, 2022. ISBN 978-989-40-0258-1. p. 22.

[152] Informações sobre o caso disponíveis na internet:<URL:http://freeross.org/category/documents/>; caso descrito no livro (RAMALHO, 2017, pp. 27-33).

[153] (RAMALHO, 2017, pp. 150-151).

[154] HARRIS, Ryan, *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Digital Investigation - The international Journal of Digital Forensics & Incident Response*, [Em linha], Vol.3, 2006, pp. 44-49, p. 45.
Disponível na internet:<URL:https://www.sciencedirect.com/science/article/pii/S1742287606000673>. [Consultado em 13/04/2025].

Estas medidas antiforenses (entre outros, anonimizadores, moedas virtuais: *bitcoin*, medidas que visam evitar o exame e análise de dados informáticos como por exemplo *data wiping*, a esteganografia, a cifragem de dados e a adulteração de dados, ataques contra perícias forenses, utilização da rede Tor) utilizadas pelos criminosos, encontram-se, pormenorizadamente, descritas no livro de David Silva Ramalho[155]. Não as reproduziremos mas aconselhamos a sua leitura para uma melhor compreensão das dificuldades e obstáculos, por vezes inultrapassáveis, com que os investigadores se deparam. A este respeito, deixaremos aqui apenas expresso o propósito destas medidas, referindo o autor "*Pode assim dizer-se que existem medidas anti-forenses específicas ou principalmente direccionadas a diferentes etapas do procedimento forense digital. Medidas que consubstanciam formas de reação da criminalidade aos conhecidos métodos de investigação criminal existentes e cujo objectivo é o de frustrar investigações em curso ou que possam vir a ser iniciadas"*[156].

Perante este cenário de evolução da criminalidade informática e sensação de insegurança, alguns Estados, visando a salvaguarda da segurança dos seus cidadãos, passaram, nas investigações criminais a permitir a utilização de tecnologias, até então, empregues apenas por *hackers* no âmbito da atividade delituosa.

Sendo a preocupação legítima, compreensível e necessária, ainda assim deverá existir uma conciliação entre a consagração de mecanismos processuais que permitam uma legítima e eficaz perseguição penal com o respeito dos direitos (liberdade e privacidade) 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[157].

Recordamos que um dos casos que trouxemos para este nosso trabalho, o *United States of America v. Robert Mclamb* estava relacionado com pornografia infantil e abordava a utilização de *malware* (o NIT do FBI) como método oculto de investigação. Ao abordar a temática relacionada com as ações encobertas (AcE) em ambiente digital, DAVID RAMALHO descreve no seu livro[158] a atuação de um agente do FBI que em 1994 participou numa investigação que tinha como objetivo detetar a prática de ilícitos relacionados com pornografia infantil na Internet. Esse agente do FBI, participou, a partir

[155] (RAMALHO, 2017, pp. 150-175).
[156] *Ibidem*, cit., p. 152.
[157] *Ibidem*, cit., pp. 202-204.
[158] *Ibidem*, cit., pp. 281-283.

de Orlando na Flórida, numa ação encoberta que decorria em salas de *chat* criadas por utilizadores do serviço AOL, fazendo-se passar por um pedófilo autointitulado de "Mikey1L". O foco da investigação eram as salas de *chat* com temas "*Boys*" e "*Preteen*", que eram frequentadas por utilizadores interessados em trocar arquivos com material pornográfico-infantil. Um caso com contornos em tudo idênticos ao que aqui trouxemos, visando, em última instância, obter provas conducentes à identificação do(s) suspeitos(s) da prática do(s) crime(s), contudo, com uma abordagem em termos de investigação diferente, ou seja, mediante a utilização de um agente encoberto digital.

Ainda que de forma sucinta, vejamos no nosso ordenamento jurídico, quais os direitos fundamentais afetados com esta última abordagem.

4.2 Direitos fundamentais afetados pelas ações encobertas em ambiente digital.

A Constituição da República Portuguesa (CRP) delimita o âmbito de atuação das forças policiais, cuja atuação em termos criminais se deve pautar com respeito pelos direitos, liberdades e garantias dos cidadãos (artigo 272.º, n.º 3 da CRP) e em conformidade com o princípio da dignidade humana e direitos fundamentais, pautando-se ainda pelo respeito dos princípios da necessidade, da exigibilidade e proporcionalidade. É também a própria CRP que admite a compressão de "direitos fundamentais" quando esteja em causa ou seja necessário salvaguardar outros direitos ou interesses constitucionalmente protegidos "*Todos esses direitos podem ser limitados ou comprimidos por outros direitos ou bens constitucionalmente protegidos (…) sendo sempre necessário fundamentar a necessidade da limitação ou compressão quando ela não se obtém por interpretação das normas constitucionais que regulam esses direitos*"[159].

A CRP permite, como sabemos formas de investigação ou recolha de prova que afetam de forma vincada Direitos, Liberdade e Garantias dos cidadãos, nomeadamente, interceções de comunicações, buscas domiciliárias, apreensão de correspondência e também AcE.

À imagem do que sucede com as demais, também o recurso à ação do AE se reveste de formalismos e requisitos legalmente exigíveis, nomeadamente, quando não seja possível a obtenção do resultado através de um meio menos intrusivo e invasivo, a sua

[159] Cf. Ac. n.º 254/99 do Tribunal Constitucional, de 4 de maio de 1999, Relator: Sousa e Brito, disponível na internet:<URL:https://www.tribunalconstitucional.pt/tc/acordaos/19990254.html>. [Consultado em 30/04/2025].

utilização deve ser proporcional quer às finalidades quer à gravidade do(s) crime(s) em investigação (previstos no catálogo do artigo 2.º do Regime jurídico das ações encobertas para fins de prevenção e investigação criminal - RJAE)[160] e, consoante o estado em que se encontre o processo, com a devida autorização do MP ou JIC. Em suma, as AcE, que tem um regime e tramitação legal específicos, são um meio de investigação que deve ser usado com parcimónia, sendo que o seu desenvolvimento deve ser objeto de aprofundado escrutínio jurisdicional.

A ação encoberta restringe os direitos à intimidade/privacidade, à autodeterminação informacional, à confidencialidade e à integridade dos sistemas técnico-informacionais (apenas no caso da ação encoberta em ambiente informático-digital), à inviolabilidade do domicílio (apenas quanto à ação encoberta "clássica" e desde que a sua realização implique a entrada num espaço que goze da tutela deste direito mediante consentimento viciado) e à liberdade de expressão[161].

Assim e apenas a título indicativo do quadro legal, quanto ao direito à intimidade/privacidade (artigo 12.º da Declaração Universal dos Direitos do Homem, no artigo 8.º da Convenção Europeia dos Direitos do Homem, artigo 17.º do Pacto Internacional dos Direitos Políticos e Civis e artigo 26.º, n.º 1 da CRP bem como aqueles que funcionam como sua garantia, nomeadamente o direito à inviolabilidade do domicílio e da correspondência no artigo 34.º e da proibição de tratamento informático de dados referentes à vida privada no artigo 35.º n.º 3, ambos da CRP), no que diz respeito à autodeterminação informacional concebida como o direito que os cidadãos têm de conhecer quem, quando e em que circunstâncias são reveladas informações sobre eles, sendo uma verdadeira proteção dos indivíduos frente á um ilimitado emprego, arquivo e retransmissão dos seus dados pessoais.

4.3 Conceito de ação encoberta em ambiente digital. Enquadramento legal no nosso ordenamento jurídico.

Foi no sentido de providenciar meios aptos a combater este tipo de criminalidade, que a UE viria a sugerir a sua implementação nas várias legislações nacionais através Diretiva

[160] Lei n.º 101/2001 de 25 de agosto (RJAE), disponível na internet:<URL:https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis>. [Consultada em 16/04/2025].

[161] NUNES, Duarte Alberto Rodrigues, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal como Instrumento de Resposta à Criminalidade Organizada*.1ª Edição. Coimbra: Gestlegal, 2019. ISBN 978-989-8951-29-8. p.830.

2011/93/UE[162] do Parlamento Europeu e do Conselho, de 13 de Dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho[163].

Pela sua importância, neste particular, aqui reproduzimos o Considerando 27 da Diretiva: " *Os responsáveis pela investigação e pela acção penal relativas aos crimes referidos na presente directiva deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a intercepção de comunicações, a vigilância discreta, inclusive por meios electrónicos, a monitorização de contas bancárias ou outras investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e a natureza e gravidade dos crimes investigados. Se for caso disso, e de acordo com a legislação nacional, tais instrumentos deverão também incluir a possibilidade de as autoridades policiais utilizarem uma identidade falsa na Internet*".

O artigo 19.º da LCc consagra o recurso a AcE em ambiente digital, com uma remissão genérica para o regime da Lei n.º 101/2001, de 25 de agosto (RJAE)[164] ou nas palavras de BENJAMIM SILVA RODRIGUES, «o legislador português, através do artigo 19.º, da LCiber 2009, veio consagrar acções encobertas em "*ambiente electrónico-digital*. Verifica-se que se afigura, nos termos do n.º 1, alíneas a) e b) o recurso às acções encobertas, previstas na Lei n.º 101/2001, de 25 de agosto […]»[165].

O RJAE já foi objeto de três alterações. A primeira através da Lei n.º 60/2013, de 23 de agosto, que aditou ao artigo 2.º o crime de tráfico de pessoas, a segunda através da Lei n.º 61/2015, de 24 de junho, que aditou, também no artigo 2.º os crimes de organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo e a terceira através da Lei n.º 2/2023, de 16 de janeiro, que completa a transposição da Diretiva (UE) 2017/541, alterando a Lei de Combate ao Terrorismo, o Código Penal, o Código de Processo Penal e legislação conexa.

Como referimos, a ação encoberta realizada em ambiente digital encontra-se regulada no artigo 19.º da LCc. Neste diploma legal, constatamos como o legislador admitiu o

[162] Disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32011L0093>. [Consultada em 16/04/2025].
[163] Disponível na internet:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32004F0068>. [Consultada em 16/04/2025].
[164] Cf. artigo 1.º da Lei n.º 101/2001. Disponível na internet:<URL:https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis>. [Consultada em 16/04/2025].
[165] RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente…, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. 1ª Edição. Rei dos Livros, 2010. ISBN 978-989-8305-06-0. p. 456.

recurso às AcE previstas e reguladas no RJAE, quando no decurso de um inquérito estejam em causa crimes previstos na LCc bem como "…*os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos*"[166].

Nota ainda para facto da Lei n.º 144/99, de 31 de agosto, Lei da cooperação judiciária internacional em matéria penal, no artigo 160.º - B, n.º 1 prever a aplicabilidade do RJAE, ao permitir a equiparação dos funcionários de investigação criminal de outros Estados quando estes desenvolvam AE em território nacional, com as mesmas prerrogativas dos funcionários de investigação criminal nacionais. Nestes termos, o catálogo de crimes permanece inalterado, por se aplicar o princípio da territorialidade, isto é, a lei nacional em solo português.

Assim, será a previsão de crimes que consta do artigo 2.º e requisitos do artigo 3.º, ambos do RJAE, que delimitam a utilização da figura do AE digital. Nestes requisitos, invocam-se os corolários constitucionais de necessidade, adequação e proporcionalidade, ínsitos no artigo 18.º, n.º 2 da CRP.

4.4 Os intervenientes das ações encobertas: agente encoberto, infiltrado, provocador e agente informador (homem de confiança e terceiros encobertos).

Para melhor percebermos este regime, importa clarificar de forma conceptual, as diferenças entre AE, agente infiltrado, agente provocador e homem de confiança.

Poderá parecer excessiva a preocupação conceptual, no entanto, avançamos que o RJAE faz uso da expressão "ações encobertas" e em nenhuma parte do diploma verificamos o emprego da expressão "infiltrado". Por outro lado, verificamos que a propósito da infiltração policial, a doutrina e a jurisprudência (esta última emprega

[166] Cf., artigo 19.º, n.º 1, al. a) e b) da Lei do Cibercrime. Disponível na internet:<URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis>. [Consultada em 19/04/2025].

indefinidamente os dois termos[167], aplicando-o em concreto ao RJAE) distinguem entre o agente provocador por um lado e, por outro, o AE e o agente infiltrado.

Vejamos estas figuras bem como a do agente informador e terceiros encobertos.

4.4.1 O agente encoberto.

A definição tradicional de AE consta do artigo 1.º, n.º 2 do RJAE. Quando referimos tradicional, pensamos naquela a que corresponde à infiltração de um polícia ou de pessoa não pertencente às forças de segurança mas que atue sob sua direção no meio criminoso. Neste diploma legal, o legislador define a ação encoberta nos seguintes termos "*Consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade*".

Assim, DUARTE NUNES citando, entre outros, ALVES MEIREIS, refere «Agente encoberto é aquele que, sem revelar a sua identidade verdadeira ou qualidade e com a finalidade de obter provas para a incriminação do suspeito ou obter uma *notitia criminis*, frequenta os meios conotados com a prática de crimes, sendo que, naquela ocasião, poderia estar qualquer outra pessoa e as coisas aconteceriam da mesma forma»[168], acrescentando, no seu entendimento, que esta conduta (sem ganhar a confiança do visado) poderá ir um pouco mais além da mera frequência de tais locais, dando como exemplo a conduta do AE que assume o papel de comprador simulado de droga (*v.g.* refere ainda outros exemplos como o de uma prostituta ou motorista de táxi que alertam outros agentes nas imediações para que estes consumem a detenção do suspeito). Em ambiente digital, refere «No plano informático-digital, a conduta do agente encoberto pode consistir no patrulhamento de sítios da Internet, *chats* ou *newsgroups* abertos ou acedido com o consentimento de um dos participantes, de redes P2P e outras "zonas de risco" do Mundo virtual, sendo que dificilmente o agente encoberto poderá adotar uma conduta de *Scheinkäufer* (potencial cliente/comprador) ou de vítima potencial, pois o modo habitual de agir no Mundo virtual é através de identidades fictícias, pelo que, nesses casos, estaremos perante um agente infiltrado; no entanto, se o agente se limitar a criar uma

[167] Neste sentido veja-se a título de exemplo Acórdãos onde se utiliza o termo "agente infiltrado": Ac. do STJ, Proc. 1/13.9YGLSB.S1, Relator Raul Borges, de 17/04/2015; Ac. STJ, Proc. 127/10.0JABRG.G2.S1, Relator Santos Cabral, de 27/06/2012.
[168] *Apud* (NUNES, 2019, p.831).

página de Internet para identificar suspeitos da prática de um dado crime (*v.g.* em matéria de pornografia infantil) sem utilizar dados identificativos fictícios, tratar-se-á de um agente encoberto»[169]. O foco aqui centra-se na ocultação da verdadeira identidade ou qualidade sem, contudo, criar uma identidade fictícia, ou seja, para o autor a partir do momento que o agente oculta a verdadeira identidade e cria uma fictícia passa a agir como um agente infiltrado.

A nível doutrinário, DAVID SILVA RAMALHO para sustentar e fundamentar os motivos pelos quais considera inútil a distinção, apresenta a definição apresentada por ALVES MEIREIS no sentido de que AE seria "um órgão de polícia criminal que «estava naquele lugar, àquela hora, como poderia estar outro agente qualquer ou outro cidadão qualquer; mas isso foi suficiente para presenciar um crime, ou para o desencadear», ou seja, «[o] 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 o crime, nem conquista a confiança de ninguém. Representa, portanto, o comum agente à paisana. Nessa medida, tratar-se-ia de um meio de obtenção de prova atípico e não proibido por lei, pelo que se encontraria abrangido pelo disposto no artigo 125.º do CPP"[170]. Em suma, diremos que para o autor a distinção não se justifica, não é relevante nem operativa, motivo pelo qual utiliza indistintamente os dois termos, aliás, em consonância com a Jurisprudência acima indicada.

4.4.2 O agente infiltrado.

Vimos como DAVID RAMALHO não distingue esta figura, no entanto, na sua obra cita SUSANA AIRES DE SOUSA e ANTÓNIO GASPAR para referir que "*Já o agente infiltrado será, em abstracto, o agente de polícia criminal ou um terceiro sob a sua direcção que propositadamente se imiscui no contexto onde ocorrem actividades criminosas e interage com o(s) suspeito(s), tendencialmente estabelecendo com este(s) relações de confiança, com o intuito de prevenir a prática de ilícitos, obter informações sobre a actividade criminosa e/ou recolher prova incriminatória, abstendo-se, porém, de provocar a prática de quaisquer ilícitos*"[171].

[169] (NUNES, 2019, p. 832).
[170] *Apud* (RAMALHO, 2017, pp.288-289).
[171] *Ibidem*, cit., p. 289.

Por sua vez, de acordo com DUARTE NUNES, «o agente infiltrado é aquele que, sem revelar a sua identidade verdadeira ou qualidade e com a finalidade de obter provas para a incriminação do suspeito ou uma *notitia criminis*, ganha a sua confiança pessoal, mantendo-se a par dos acontecimentos, infiltrando-se no meio criminoso em causa (*v.g.* numa organização criminosa), acompanhando a execução dos factos e praticando atos preparatórios ou mesmo de execução (se necessário), mas sem o determinar à prática de crimes, atuando de forma prolongada no tempo e, tratando-se de um elemento das autoridades policiais, utilizando uma identidade fictícia. No plano informático-digital, a conduta do agente infiltrado consistirá em frequentar o Mundo virtual, utilizando identidade fictícia, ganhando a confiança dos visados, mantendo-se a par dos acontecimentos e acompanhando a execução de factos e praticando atos preparatórios ou de execução (se necessário), mas sem determinar ninguém à prática de crimes»[172].

Por sua vez ARMANDO RAMOS, citando MANUEL COSTA ANDRADE refere «Têm-se por agente infiltrado aquele que não se limitando a ocultar a sua verdadeira identidade consegue granjear no suspeito uma aproximação de confiança e solidariedade, sem interferir com o resultado pretendido, isto é, visa exclusivamente a recolha de prova sem incitar ou precipitar o *actus delitual*»[173]. Este mesmo autor, refere que a doutrina encarregou-se de estabelecer a figura do agente infiltrado com alguma similitude com a de AE, existindo, contudo, quem não encontre disparidade na utilização destes dois vocábulos e os utilize de forma indistinta, dando como exemplo o parecer do Conselho Consultivo da PGR n.º I001462001, Relator Maria João Carvalho, de 16-05-2002, onde refere "[c]onsidera-se actuação de agente infiltrado ou encoberto a que é desenvolvida por funcionário de investigação criminal…"[174].

Para quem defende a distinção destas figuras, se bem entendemos, a diferença reside no facto da ação do AE ser passiva, isto é, está presente, visualiza o desenrolar do *modus operandi*, no entanto, nunca interfere ou ganha a confiança de quem quer que seja, ao passo que o agente infiltrado assume uma conduta ativa, ou seja, ganha a confiança e amizade dos criminosos com quem interage, sem contudo realizar atos conducente à provocação do crime. A respeito desta distinção ARMANDO RAMOS, suscita algumas questões, que se nos afiguram pertinentes, nomeadamente, a que ocorre quando um investigador criminal, ou terceiro, que presencie a prática de um crime (visualizando o

[172] (NUNES, 2019, pp. 832-833).
[173] *Apud* (RAMOS, 2022, p. 54).
[174] (RAMOS, 2022, p. 54).

acontecimento e desenrolar do *delictus* sem interferir no resultado) em seu entender, que acompanhamos, não atua como AE mas sim como mera testemunha. Relativamente ao agente infiltrado, refere, como também defendem outros autores, que o mesmo ganha a confiança e amizade com quem interage, mas sem realizar atos conducentes à provocação do crime, para referir que também o AE não procede de tal forma, pois caso atuasse com condutas provocatórias deixaria de estar no papel de AE, passando a agente provocador e, consequentemente a inquinar a prova obtida e violando a lei que sustenta a sua ação[175].

Nestes termos, até por assim se encontrar definido em termos legais (RJAE), estamos mais inclinados para a o uso da expressão "agente encoberto", acompanhando DAVID RAMALHO no que considera ser uma desvantagem de utilização dos dois termos, justificando a génese da distinção com o facto de o conceito de AE, por contraposição ao de agente infiltrado, ter surgido na vigência dos artigos 59.º e 59.º-A do Decreto-Lei n.º 15/93, altura em que, não só a lei não utilizava o termo *encoberto*, como utilizava o termo *infiltrado* (referindo-se ao funcionário ou terceiro infiltrados na epígrafe do artigo 59.º-A n.º 3)[176].

4.4.3 O agente provocador.

Constatamos que a fronteira entre AE e agente provocador é muito ténue e tentaremos, de acordo com definições que iremos expor, delimitar o espaço de ação que nos permita aferir o momento em que nos encontramos na presença de um e outro.

Nas palavras de DAVID RAMALHO, que acaba por resumir em síntese o pensamento de outros autores, "*Em síntese, o agente provocador é o órgão de polícia criminal ou um terceiro sob a sua direcção que determina ou estimula outrem à comissão de um crime que de outro modo não seria por si praticado, geralmente motivado pela vontade de facilitar a recolha de prova da ocorrência do facto criminoso*"[177]. O autor coloca o foco no papel decisivo e interventivo da atuação na génese e comissão do crime, acrescentando que o que distingue esta figura do agente encoberto ou infiltrado (considera como vimos que ambas reconduzem-se à mesma figura) se deve ao facto do agente provocar uma intenção da prática de um crime, até então inexistente[178]. No mesmo sentido DUARTE NUNES, refere «o agente provocador é aquele que, sem querer o crime em si mesmo e com

[175] *Ibidem*, cit., p. 55.
[176] (RAMALHO, 2017, p. 290).
[177] *Apud* (RAMALHO, 2017, p. 291).
[178] *Ibidem*, cit., p. 291.

a finalidade de sujeitar o visado a um processo penal e, consequentemente, a uma pena, convence outrem a cometer um crime que, não fosse a atuação do agente provocador, jamais cometeria. Ao nível da comparticipação criminosa, o agente provocador será, consoante a sua atuação concreta, instigador ou mesmo autor mediato. No plano informático-digital, a conduta do agente provocador consiste em frequentar o Mundo virtual, com utilização de uma identidade fictícia, e convencer outrem a cometer crimes que, não fosse a sua atuação, jamais cometeria»[179].

Assim, essencial é estabelecer o que se entende por provocação e nesse sentido, em resposta, GERMANO MARQUES DA SILVA afirmou "*a provocação não é apenas informativa, mas sobretudo formativa, não revela o crime e o criminoso, mas cria o próprio crime e o próprio criminoso e, por isso, é contrária à própria finalidade da investigação criminal, uma vez que gera o seu próprio objecto*"[180].

No plano da validade da prova que venha a ser obtida, que não abordaremos neste trabalho, sempre diremos que uma ação encoberta que possa ser considerada como ação provocatória de um crime não pode valer como meio válido de obtenção de prova, o que implica a inexistência de qualquer prova do crime provocado nos termos previstos nos artigos 126º, nº 2, al. a) do Código de Processo Penal e 32º, nº 8 da Constituição da República Portuguesa[181].

4.4.4 Agente informador e terceiros encobertos.

«A figura do agente informador é, por vezes conotada com a semblante do agente encoberto. MANUEL DA COSTA ANDRADE define agente informador como *homens de confiança* onde se inserem tanto os particulares (pertencentes ou não ao submundo da criminalidade) como agentes das instâncias formais, nomeadamente da polícia. O autor acrescenta que o recurso ao agente informador configura um meio enganoso e consequentemente um método proibido de prova previsto no artigo 126.º, n.º 2, alínea a) do CPP. Contudo este ilustre Professor admite o uso desta figura desde que não exista provocação e se destine a "*finalidades exclusiva ou prevalentemente* preventivas". Já SUSANA AIRES DE SOUSA entende que a expressão "*homens de confiança*", usados quer na doutrina quer na jurisprudência, é um conceito extensivo abrangendo "*todas as*

[179] (NUNES, 2019, pp. 833-834).
[180] *Apud* (RAMOS, 2022, p. 64); *Apud* (RAMALHO, 2017, p.292).
[181] Cf. Acórdão da Relação do Porto de 22/01/2014. Disponível na internet:<URL: https://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/5ad35fe25bc9cc8380257c77003db568?OpenDocument>. [Consultado em 19/04/2025].

testemunhas que colaboram com as instâncias formais de perseguição penal, tendo como contrapartida a promessa da sua confidencialidade da sua identidade e actividade"»[182].

A forma como entendemos esta figura, estará relacionada com a por vezes designada figura das "fontes", ou seja, estes *homens de confiança* como sendo terceiros que não tem que ser necessariamente do mundo criminal, com quem os investigadores mantém relações de confiança recíprocos, a quem aqueles prestam informações que poderão vir a revelar-se importantes em sede de investigação criminal, inclusive mediante a recolha de prova que possam vir a realizar. De acordo com o tipo de atuação e requisitos casuísticos verificados, poderemos estar perante os terceiros previstos no RJAE (se estiverem em dependência funcional e material da PJ e com permissão das autoridades judiciárias, MP ou JIC) e nesses casos estaremos perante uma ação encoberta. Caso não se mostrem cumpridos estes requisitos não estaremos perante a situação de um agente informador como AE. A jurisprudência tem sido unânime no entendimento que um terceiro que revele à polícia a prática iminente de um crime ou de quem foram os seus autores, não atua na qualidade de um AE[183]. A atuação deste terceiro em termos processuais poderá vir a ocorrer na qualidade de denunciante (caso não recorra ao anonimato) ou eventualmente como testemunha.

Para finalizar estes conceitos refere DUARTE NUNES que «o "homem de confiança" é uma pessoa não pertencente às forças policiais (podendo pertencer ao *milieu* criminoso) e que coopera com estas (sob a direção destas), assumindo uma conduta que, consoante a situação concreta, configurará a atuação de um agente encoberto, infiltrado ou provocador. No plano informático-digital, a conduta do "homem de confiança" corresponderá à atuação do tipo de agente que "encarnar»[184].

4.5 (In)admissibilidade do agente encoberto e do agente infiltrado.

Vimos as diferentes posições relativamente à (in)existência da distinção entre AE e agente infiltrado e será de acordo com a sustentada que veremos a forma como se legitima a sua admissibilidade.

---

[182] *Apud* (RAMOS, 2022, p. 57).
[183] Assim decidiu o TRL *"[s]ó actua como agente provocador quem actua de forma a criar o próprio crime ou instiga a respectiva prática. No caso dos autos o arguido H. criou o próprio crime e a testemunha limitou-se a revelá-lo informando a PJ de que o crime estava a ser preparado e, como previsto, veio a ser consumado.*" Ac. do TRL, Proc. 6919/2003-5, Relator Ana Sebastião, de 15-06-2004. No mesmo sentido o Ac. TRP, Proc. 2039/14.0JAPRT.P1, Relator José Carreto, de 07-07-2016.
[184] (NUNES, 2019, p.835).

Nestes termos, "*No direito português, o agente infiltrado é admissível à luz da Lei n.º 101/2001 e, no caso das ações encobertas em ambiente informático-digital, à luz do artigo 19.º da lei n.º 109/2009. E o agente encoberto é admissível à luz do artigo 125.º como meio de obtenção de prova atípico, não sendo aplicável, pelo menos diretamente, o regime da Lei n.º 101/2001…*"[185]. A corroborar a admissão do agente encoberto como meio de obtenção de prova atípico, em nota de rodapé, o autor cita MARCOLINO DE JESUS, FERNANDO GONÇALVES/MANUEL JOÃO ALVES/GUEDES VALENTE, ALVES MEIREIS, GUEDES VALENTE, entre outros. Relativamente à inaplicabilidade direta do regime da Lei 101/2001, o autor refere GUEDES VALENTE referindo que o mesmo para fundamentar a sua posição recorreu a uma distinção entre AE e "polícia à paisana" (com o mesmo entendimento ISABEL ONETO e DANIEL SILVA), referindo em nota de rodapé que «O agente encoberto, tal como o "polícia à paisana", circula por locais relacionados com a prática de crimes (*v.g.* tráfico de estupefacientes, lenocínio, crimes contra o património, etc.) com a finalidade de detetar a prática de crimes e identificar os seus autores. No entanto, o agente encoberto, diversamente do que faria o mero "polícia à paisana", não detém necessariamente de imediato o criminoso e poderá agir como alvo do criminoso (*v.g.* passando-se por prostituta, mero transeunte) ou como cliente simulado ou potencial cliente (*Scheinkäufer*)»[186].

De acordo com a sua interpretação, pese embora a definição da ação encoberta conste do artigo 1.º, n.º 2, da Lei n.º 101/2001 e permita incluir o AE, numa interpretação global do diploma e da diferença bastante acentuada entre AE e infiltrado (a maior reside na utilização de identidade fictícia por parte do infiltrado), faz o autor concluir que este diploma não se refere ao AE.

O recurso à figura do AE e infiltrado, para além de controverso, suscita questões de utilidade principalmente no combate à criminalidade organizada, que recorre, como já aqui enfatizámos, cada vez mais a sofisticados recursos tecnológicos.

Relativamente às AcE em ambiente digital (ou informático-digital) este método tem obtido algum sucesso na repressão de alguns fenómenos criminais (*v.g.* pornografia infantil e pedofilia *online*, jogo ilícito, tráfico de estupefacientes), sendo de realçar que nas investigações na *Dark web*, a sua utilização tem permitido ultrapassar todas as questões associadas ao anonimato de utilizadores, na medida em que o agente infiltrado

[185] *Apud* (NUNES, 2019, p.838).
[186] *Ibidem*, cit., p. 838 (nota de rodapé -2832).

ao "integrar-se" nessa comunidade fechada interage com os criminosos, ganha a confiança destes e são os próprios que, invariavelmente, acabam por ceder elementos que levam à sua posterior identificação bem como das suas vítimas.

Para aqueles que não distinguem as figuras, como bem se entende, o regime aplicável será o da Lei n.º 101/2001 e Lei n.º 109/2009 (artigo 19.º).

4.6 O agente encoberto informático em Espanha.

Optamos, neste estudo, por abordar o exemplo espanhol, não só pela proximidade mas também pelos hábitos sociais e culturais que nos aproximam.

Atualmente o conceito de AE em Espanha é altamente regulamentado, existindo grande preocupação pelo respeito pelo princípio da legalidade, controlo judicial e proteção dos direitos humanos. As operações devem ser previamente autorizadas por um juiz, e os agentes atuam com limites estabelecidos na lei, registando e documentando detalhadamente todas as ações.

As alterações legislativas revelam a preocupação com o aumento da cibercriminalidade, aliás expressas na *Estrategia Nacional de Ciberseguridad 2019* publicada pela ordem PCI/487/2019[187]. Nesta estratégia, a cibercriminalidade surge definida (Capítulo 2 - *Las amenazas y desafíos en el ciberespacio*) como "*El término Cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas*".

Nesta estratégia, no Capítulo 4 (*Líneas de acción y medidas*), a terceira linha de ação tem por objeto "*Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio*". Para atingir esse desiderato, uma das medidas contempladas (a primeira das medidas indicadas nessa terceira linha de ação) é reforçar o quadro jurídico para responder eficazmente à cibercriminalidade, tanto no que diz respeito à definição de tipos penais como à regulação de medidas adequadas de investigação[188]. Esta última é que releva para o nosso estudo.

[187] Disponível na internet:<URL:https://www.boe.es/buscar/act.php?id=BOE-A-2019-6347&p=20190430&tn=0>. [Consultada em 19/04/2025].

[188] Tradução nossa do original: "*Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación*".

Assim, veremos até que ponto esta linha de ação tinha sido plasmada no *Anteprojeto da Ley de Enjuiciamiento Criminal de 2019*[189] e quais foram as alterações que sofreu no que diz respeito à regulação do AE informático, uma das diligências de investigação tecnológica empregues contra algumas das formas de cibercriminalidade existentes.

O AE informático, na atual conceção normativa do direito espanhol, não é mais do que uma especialidade do AE consagrado na luta contra o cibercrime. Só com as alterações ocorridas em 2015 é que o legislador espanhol regulou esta figura (*Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*[190] *e Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito*[191]). Com as alterações, foi introduzido na *Ley de Enjuiciamiento Criminal*[192] (*LECrim*) o artigo 282 bis, n.º 6, que passou a dispôr*: "El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a*".

Recentemente a Jurisprudência espanhola definiu o AE como "um funcionário das forças policiais que atua na clandestinidade com uma identidade fictícia com a finalidade de prevenir ou reprimir a prática de crimes"[193].

O ordenamento jurídico espanhol criou, desta forma, uma figura especial para levar a cabo investigações nos denominados "*canales cerrados de comunicación*" e habilitada a transmitir nesses canais ficheiros informáticos ilícitos. Encontramos aqui algo muito próximo ao AE digital no ordenamento jurídico português. O AE informático, no ordenamento jurídico espanhol, pode ser definido como "*…un agente de la policía judicial que, al igual que el agente encubierto, actuará com una identidade supuesta,*

[189] Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/210126%20ANTEPROYECTO%20LECRIM%202020%20INFORMACION%20PUBLICA%20%281%29.pdf>. [Consultada em 19/04/2025].
[190] Disponível na internet:<URL:https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725>. [Consultada em 19/04/2025].
[191] Disponível na internet:<URL:https://www.boe.es/buscar/act.php?id=BOE-A-2015-4606#dfprimera>. [Consultada em 19/04/2025].
[192] Disponível na internet:<URL:https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. [Consultado em 19/04/2025].
[193] PUIGVERT, Sílvia Pereira / PONZ, Francesc Ordóñez (Directores) / ZAMORA, María Jesús Pesqueira (Coordinadora), *Investigación Y Processo Penal en el Siglo XXI Nuevas Tecnologías Y Protección de datos*, Editorial Arazandi, 2021. ISBN 978-84-1390-520-4. p. 151.

pero, a diferencia de este último, no interactuará fisicamente com el investigado sino telemáticamente y por medio de canales cerrados quien, además, para ganarse la confianza del investigado, quedará facultado para enviar archivos con contenido ilícito[194].

No âmbito de intervenção, destacamos que o escopo de atuação do AE informático é mais amplo que o AE (tradicional). Podem ambos ser empregues numa resposta à criminalidade organizada. Por outro lado, o AE informático poderá intervir na investigação de todo o tipo de crimes dolosos, cuja moldura penal seja igual ou superior a 3 anos de pena de prisão ou quando se trate de crimes cometidos através de meios informáticos. O alargamento do âmbito de atuação do AE informático reforça a importância e relevância que esta figura assume no combate ao cibercrime.

Ainda assim, tal como acontece no nosso ordenamento jurídico, para os autores a que temos vindo a fazer referência ao ordenamento jurídico espanhol, o legislador descuidou-se na regulação de alguns aspetos desta figura. A pouca regulação atual acerca do AE informático omite, em termos gerais, várias questões de maior importância prática, destacando: a delimitação das funções preventivas e investigações preventivas proibidas pelo ordenamento jurídico espanhol, os requisitos e oportunidade do momento para prolação do auto que autoriza a diligência de investigação, a incorporação das atas no processo e o conceito de canal fechado de comunicações[195].

No âmbito da proposta de *Anteproyecto da Ley de Enjuidiciamento Criminal de 2020*[196], na exposição de motivos (XLVI, p.54) descreve-se a ação encoberta como uma medida especial de investigação introduzida pela *Ley Orgánica 5/1999* (*la entrega vigilada y al agente encubierto*), bem como o sucedâneo tecnológico deste conhecido como "*agente encubierto informático*", introduzido pela legislação em vigor da *Ley orgánica 13/2015*.

Na mesma exposição de motivos (XLVII, p.55) faz-se referência ao AE. Destaque ainda, nesta proposta (p. 120 por referência ao índice), para o facto de dedicar um capítulo próprio, no Título VII, relativo às ações encobertas. Neste Título o AE é regulado de forma separada (Capítulo II) e o AE informático (Capítulo III). Se atentarmos que foram

---

[194] *Ibidem*, cit., pp. 151-152.
[195] *Ibidem*, cit., pp. 152-153.
[196] Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/210126%20ANTEPROYECTO%20LECRIM%202020%20INFORMACION%20PUBLICA%20%281%29.pdf >. [Consultada em 19/04/2025].

dedicados 5 artigos completos, constatamos o interesse e importância dados a esta última figura. Destaque ainda para a introdução neste diploma, através do artigo 512 de limites objetivos e subjetivos, por forma a, para ampliar o âmbito da investigação a factos distintos daqueles que suportaram a realização da diligência ou para ampliar a investigação a outros suspeitos, mostra-se necessária uma nova autorização judicial.

O âmbito de atuação permanece praticamente inalterado, o AE informático poderá intervir na investigação de todo o tipo de crimes dolosos, cuja moldura penal seja igual ou superior a 3 anos de pena de prisão ou que se trate de crimes cometidos através de meios informáticos.

5. RECURSO AO *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM PROCESSO PENAL

As origens do *malware* remontam a dois casos que causaram múltiplas infeções nos computadores de vários utilizadores, o *Melissa* (em 1999) e o *LoveLetter* (em 2000). Foram difundidos por email, sendo que o *LoveLetter* tinha a particularidade de constar de um anexo de email infetado que sendo aberto, fazia com que o *malware* substituísse vários tipos diferentes de arquivos no computador, reenviando-se automaticamente para outras pessoas da lista de contactos de endereços de email do utilizador[197].

Talvez seja importante recordar que foi para fazer face ao aumento das interações dos cidadãos com a tecnologia e ao aumento da quantidade de informação armazenada em sistemas informáticos, em movimento e através das redes (pensemos na troca de arquivos de pornografia infantil), que diversos países, para fazer face ao aumento da cibercriminalidade e para contrariar as técnicas antiforenses utilizadas por agentes e grupos criminosos, começaram a utilizar como meio de obtenção de prova o *malware*.

Foi através destes novos meios de obtenção de prova que as AJ e os OPC, passaram a dotar as investigações destes "*novos meios*" e técnicas associadas, procurando desta forma nivelar um "*jogo*" (do gato e do rato) que, infelizmente, arriscamos dizer, tem vindo a pender para o lado dos cibercriminosos.

[197] BARLOWEM, Bill *et al.*, *Microsoft Security Intelligence Report: Special Edition*, 2012, p.4. Disponível na internet:<URL:https://www.microsoft.com/pt-br/download/details.aspx?id=29046>. [Consultado em 24/04/2025].

5.1 Conceito *Malware* e técnicas adotadas pelos OPC.

Em termos conceptuais, acolhemos a definição de FILIOL que DAVID RAMALHO traduziu nos seguintes termos: "*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*"[198]. Encontramos em literatura diversa várias definições, como por exemplo aquela que foi avançada por BOLDT, como "*um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça*"[199].

Em Portugal, o conceito mais utilizado a nível doutrinário é a busca *online* e cavalos de Tróia (*Trojan Horses* ou, simplesmente, *Trojans*).

Neste sentido, devemos ainda ter em conta, como refere RAMALHO, que pese embora o termo Cavalo de Tróia seja o mais utilizado para referir *malware*, na verdade ele é apenas um dos vários tipos de *malware* que podem ser utilizados no âmbito de investigações criminais em ambiente digital. O autor dá como exemplo, as *logic bombs*, o *spyware*, os *rootkits*, os vírus e *worms* e as *blended threats* (ameaças mistas) que utilizam mais de um tipo de *malware*, que nos absteremos de descrever e pormenorizar[200].

O termo *malware* resulta da contração do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático)[201]. Sendo empregue por forças policiais, a doutrina atribui-lhe diversas designações, nomeadamente, "*goverment hacking*"," *network investigative Technique (NIT)*", "*policeware*", "*hacking legal*", "*hacking by law enforcement*", "*lawful hacking*", "*hacker policial*"[202].

---

198 *Apud* (RAMALHO, 2013, p. 202). [Consulado em 16/04/2025].

199 BOLDT, Martin, *Privacy-Invasive Software*, Karlskrona: Blekinge Institute of Technology, 2010, p. 11. ISBN 978-91-7295-177-8. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diva-portal.org/smash/get/diva2:835533/FULLTEXT01.pdf>. [Consultado em 17/04/2025].

200 (RAMALHO, 2013, p.202); Relativamente a funcionalidades e formas de instalação CAMPOS, Juliana Filipa Sousa, *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Almedina, 2021. ISBN 978-972-40-9021-4. pp. 37-40.

201 (RAMALHO, 2013, p. 201).

202 A este respeito, *vd.*, OHM, PAUL, "*The Investigative Dynamics of the Use of Malware by Law Enforcement", William & Mary Bill of Rights Jounal*, Vol. 26, n.º 2, 2017, pp. 303-334, p.311, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1836&context=wmborj>. [Consultado em 24/04/2025]; GUTHEIL, Mirja *et. al.*, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices: Study for the LIBE Committee*, 2017, p.44, disponível na internet:<URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>. [Consultado em 24/04/2025]; PRADILLO, Juan Carlos Ortiz, *"Hacking" legal al servicio de la*

A este respeito e verbalizado por um Procurador da República, retivemos o termo "*benware*", utilizado para referir o uso deste tipo de *software* por parte das forças policiais. Utilizando o mesmo tipo de desconstrução, podemos dizer que se juntarmos a contração do adjetivo *benevolent* (benévolo, bem intencionado ou gentil) com o uso do substantivo *software* (programa informático), teremos o termo *benware*, que será, em termos valorativos (ainda que insidioso e intrusivo), mais adequado para um instrumento utilizado por órgãos de polícia criminal[203]. O propósito de utilização é valorado e reconhecido e desta forma afastamos a conotação negativa associada.

Não devemos perder de vista que, entre outros, o objetivo da utilização deste tipo de *software* por parte dos órgãos de polícia criminal, visa obter dados, comunicações, históricos de acessos e páginas visitadas na internet (inclusivamente os acessos à nuvem e respetivas credenciais), por vezes a monitorização em tempo real por ativação por exemplo, da *webcam* ou do microfone do computador visado (*hardware*), por forma a encontrar provas do envolvimento na prática de crimes, ou seja, dotar as investigações criminais de meios aptos a igualar ou superar as vantagens tecnológicas dos criminosos.

Sem entrarmos muito em pormenores técnicos, acrescentamos apenas que o processo de instalação do *malware* por parte dos OPC decorre, invariavelmente, sem o conhecimento e consentimento do visado, através de três métodos: via suporte físico removível (*v.g.* uma pen UBS), via *web browser* (também denominado de *drive-by-download*, em que o utilizador acede a uma página *web* pensando que é inofensiva, quando na realidade tem código malicioso que deteta vulnerabilidades no sistema informático do visitante, infetando-o com *malware;* outra variante é o *malvertising* que mais não é do que um *download* automático do *malware* quando o visado inadvertidamente clica num *link* disfarçado de publicidade) e por via de um download voluntário efetuado pelo visado sem que disso se aperceba (*v.g.* o download de ficheiros que constam como anexos de correio electrónico, programas executáveis ou através de falsas atualizações de *software* legítimo)[204].

---

investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquência informática, Revista de Derecho y Proceso Penal, n.º 26, ano 2011-2, Navarra: Editorial Aranzadi, 2011.pp.71-72; e PFEFFERKORN, Riana, *Security Risks of Government Hacking, The Center of Internet and Society*, 2018, disponível na internet:<URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cyberlaw.stanford.edu/content/files/sites/default/files/publication/files/2018.09.04_security_risks_of_government_hacking_whitepaper.pdf>. [Consultado em 24/04/2025].

[203] No decorrer do nosso estudo, encontramos posteriormente referência a este termo cf. ARMANDO, Dias Ramos, *O Agente Encoberto…*, cit., (nt. 12) p. 19.

[204] A este respeito e de forma detalhada (RAMALHO, 2013, p. 205-207).

«O uso de *malware* pelas forças policiais ganhou especial dimensão no ano de 2001, altura em que foi divulgada a existência do *malware* norte-americano *Magic Lantern*, tendo mais tarde dado origem ao *Computer and Internet Protocol Addresss Verifier* (CIPAV)[205], e que consistia num *keylogger*[206] instalado no computador de indivíduos – localizados ou não nos EUA – suspeitos de estarem relacionados com atividades criminosas, em particular de natureza terrorista.

Porém, a modalidade mais invasiva de *malware*[207] publicamente conhecida a ser utilizada por forças policiais viria a ser divulgada, com um grande impacto na comunicação social[208], na Alemanha, em 2011, por um grupo *hacker* intitulado de *Chaos Computer Club*. Este programa, entretanto vendido também à Áustria, viria a ser apodado de *Bundestrojaner* e consiste numa espécie de *malware* enviado para o computador do suspeito sob a forma de uma comum atualização de *software* e que, após instalação, permite gravar as chamadas Skype, monitorizar toda a atividade do suspeito na Internet, gravar as palavras-passe por ele inseridas e, inclusivamente, ativar o *hardware* do computador do visado, utilizando os seus microfones e a *webcam* para gravar sons e tirar fotos que "subsequentemente" serão enviadas para as autoridades»[209].

Já aqui aludimos à sugestão do Parlamento Europeu e do Conselho no âmbito do Considerando 27 da Diretiva 2011/93/UE[210] e pese embora a utilização deste tipo de *software* suscite questões complexas associadas ao princípio da lealdade e da proporcionalidade face ao conflito com o direito à reserva da intimidade da vida privada

[205] Cf. RAMALHO (nota de rodapé 209), Este *software* viria a ser divulgado em 2007 através da publicitação de um pedido de mandado apresentado pelo Agente Especial do FBI Norman Sanders no âmbito de um processo em que se procurava detetar o autor de várias ameaças de bomba.
[206] Cf. RAMALHO, Trata-se de um *software* que visa gravar informação que identifica as teclas premidas pelo utilizador de um sistema informático, com vista à monitorização e documentação da atividade empreendida neste, bem como à obtenção das palavras passe e outras informações relevantes que tenham sido introduzidas através do teclado.
[207] Cf. RAMALHO, Não incluímos aqui, naturalmente, os já célebres vírus *Stuxnet* e *Flame*, uma vez que o seu âmbito de aplicação material se reporta à espionagem e não à investigação criminal.
[208] Cf. RAMALHO, Já anteriormente, em 2008, o Tribunal Constitucional Alemão declarara inconstitucional a Lei da Renânia Norte-Vestefália que introduzia a utilização de *malware* como meio de obtenção de prova, fundamentando-o, entre outros motivos, no facto de esta não respeitar o princípio da proporcionalidade. Simultaneamente, o Tribunal reconheceu o direito fundamental à garantia da confidencialidade e integridade dos sistemas informáticos *(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).
[209] RAMALHO, David Silva, *A investigação Criminal na Dark Web*. Revista de Concorrência e Regulação. Ano IV, Número 14/15 (2013), (pp. 383-429), pp.416-417. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.concorrencia.pt/sites/default/files/imported-magazines/CR14_15_-_Victor_Castro_Rosa.pdf>. [Consultado em 24/04/2025].
[210] Supra, p.79.

(que não abordaremos), a verdade é que, a sua utilização em diversos ordenamentos jurídicos se tem revelado crescente.

Se bem entendemos a posição de DAVID SILVA RAMALHO, pese embora o autor reconheça a existência de norma legal habilitante para recurso ao *malware* no plano do direito constituído, coloca reservas à sua utilização da *Dark Web*, constatando que esta teria que se revestir de peculiaridades que poderiam comprometer a sua admissibilidade no plano legal e constitucional[211]. Resumidamente coloca a diferença, por um lado, referindo que o *malware* geralmente utilizado por algumas forças policiais pressupõe o conhecimento prévio da identificação do suspeito e o envio do *software* dissimulado como atualização de um outro programa, ao contrário do que sucede na *Dark Web*, onde as características do anonimato dificultam, e muitas vezes inviabilizam esse conhecimento da identidade do suspeito. Neste segundo caso, até pelo conhecimento que os utilizadores deste tipo de redes possuem (*Tor* ou *Freenet*), mostra-se muito mais difícil "convence-los" a descarregar voluntária e inadvertidamente *software* enviado por forças policiais. A solução passa, literalmente, por enganá-los, ou seja, implantar o *software* em ficheiros disfarçados com nomes sugestivos de conteúdo ilegal, divulga-los em *websites* e fóruns dedicados de partilha, na esperança que algum utilizador incauto faça *download* do mesmo.

O procedimento descrito, «… assemelha-se em muito àquele utilizado pelo FBI, em 2008, no caso das *hyperlink sting operations*, embora, neste caso, esse método tenha sido utilizado na *Surface Web*. As *hyperlink sting operations* consistem na publicitação, por parte de um órgão de polícia criminal, de *hyperlinks* que supostamente dariam acesso a conteúdo de natureza pedo-pornográfica, mas que, na realidade, uma vez acedidos, apenas servem para dar conhecimento ao FBI do endereço de IP da ligação a partir da qual partiu a comunicação. Ora, a possibilidade de estes ficheiros e *hyperlinks* serem reenviados entre vários cibernautas, sem qualquer referência ao seu conteúdo, por via de vários tipos de comunicações eletrónicas (pense-se, por exemplo, no utilizador que copia o *link* ou reenvia o ficheiro com o título alterado para um terceiro sem fazer menção ao seu conteúdo), permite que o acesso aos mesmos nem sempre manifeste uma intencionalidade de acesso ao conteúdo ilícito, mas antes se traduza no mero acesso a um *hyperlink* ou no *download* de um ficheiro sem conhecimento do seu conteúdo»[212].

[211] RAMALHO, David Silva, *A investigação Criminal na Dark Web*…, cit., p.417.
[212] RAMALHO, David Silva, *A investigação Criminal na Dark Web*…, cit., p.418.

Referindo que uma atuação deste tipo poderia revelar uma atividade de natureza provocadora (comparável à do agente provocador), com potencial excessivamente gravoso, elevados índices de falibilidade e potencialmente violadora de princípio da proporcionalidade (no confronto com os interesses sacrificados e aqueles que se visa salvaguardar), concluí dizendo que o *malware* na *Dark Web* não poderá ser utilizado.

Nesta dicotomia entre o significado e alcance que o uso do *malware* acarreta no âmbito de investigações criminais e eventuais conflitos que surgem com a forma como é utilizado em termos processuais, com contornos potencialmente geradores de graves restrições fundamentais, é chegado o momento de analisarmos o nosso ordenamento jurídico e vermos como este meio oculto se integra e adequa em termos processuais.

5.2 O uso de *malware* como meio de obtenção de prova em processo penal.

O ordenamento jurídico Português não faz qualquer referência expressa sobre a utilização de *malware* como meio de obtenção de prova, motivo pelo qual existe divergência doutrinária a este respeito, havendo quem, por um lado, considera a existência de norma habilitante e por outro, aqueles que pugnam pela sua inexistência.

Para melhor sustentarmos a nossa posição, consideramos preferível, descrever num primeiro momento estas posições.

5.2.1 Defensores de existência de norma habilitante.

Na ausência de referência expressa, tem sido a doutrina e jurisprudência, na avaliação da admissibilidade e legitimidade, que a vem reconduzindo aos meios de obtenção de prova que constam na LCc. A recondução é feita, por vezes, com fundamento na aplicação direta do regime da interceção de comunicações, previsto no artigo 18º da LCc; noutras com base no regime da interceção de comunicações e simultaneamente com o regime das buscas; outros ainda, com base na aplicação do regime da pesquisa de dados informáticos, previsto no artigo 15º da LCc; e por fim, os que legitimam a sua utilização por recurso à figura do AE em ambiente digital, previsto no artigo 19º, n. º 1 da LCc.

Segundo DAVID RAMALHO, existe consagração legal e encontra-se expressa na LCc: "*Entendemos que o uso de malware como meio de obtenção de prova está já consagrado no ordenamento jurídico nacional, em particular no artigo 19.º, n.º 2, da Lei do Cibercrime*"[213].

[213] (RAMALHO, 2017, p. 338).

Para o autor, os "*meios e dispositivos informáticos*", referidos no n.º 2, não se subsumem a qualquer um dos meios de obtenção de prova previstos na nossa legislação. Pelo contrário, a norma surge para colmatar a insuficiência dos demais meios processuais existentes e, em consequência, permite a utilização destes novos meios e dispositivos informáticos[214]. Não se trata de dispositivos eletromagnéticos, acústicos, mecânicos ou outros utilizados no conceito de interceção da alínea e) do artigo 2.º da LCc, mas sim de um outro meio que visa recolher prova de um modo inadmissível até à sua entrada em vigor[215]. Estamos, segundo este autor, perante "*meios e dispositivos que operam de modo materialmente semelhante à figura do agente encoberto - em particular ao agente encoberto em ambiente digital - e que devam ser utilizados quando a própria ação encoberta e os demais métodos ocultos forem incapazes de dar respostas às exigências da investigação. Trata-se […] da consagração do hacking e da utilização […] de malware como método oculto de investigação criminal em ambiente digital*"[216].

Acrescenta ainda o fundamento do uso de uma terminologia semelhante por parte de diplomas de outros ordenamentos jurídicos, a saber: "meios técnicos", no § 5.2 (11) da Lei de Proteção da Constituição da Renânia do Norte-Vestefália; "dispositivos técnicos", no artigo 706-102-1 do CPP francês; e "dispositivos de vigilância de dados", no artigo 6.º do *Surveillance Devices Act* australiano[217].

Importa recordar que, nem sempre, DAVID RAMALHO defendeu esta posição de forma tão manifesta. Em 2013, quando se pronunciou pela primeira vez sobre esta questão, defendeu que, ao concluir-se que o n.º 2 do artigo 19.º da LCc previa o uso de *malware*, não se podia concordar com os moldes em que o mesmo tinha sido consagrado. Considerou o autor que o dever de precisão legal não seria compatível com a mera criação de um meio de investigação cujo funcionamento e finalidade não eram (são) referidos na própria norma que os prevê. Acrescentou que a "*utilização de malware não se compadece com uma mera referência à sua necessidade, seguida de 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*"[218]. Nestes termos, a previsão legal devia ser reforçada com a necessária qualidade de Lei, como já havia referido o Tribunal Europeu dos Direitos Humanos (TEDH) em outras ocasiões. Concluiu, assim, pela

[214] *Ibidem*, cit., p. 344.
[215] *Ibidem*, cit., p. 344.
[216] *Ibidem*, cit., p. 346.
[217] *Ibidem*, cit., p. 346.
[218] Cf. (RAMALHO, 2013, p. 234).

inconstitucionalidade da norma, por violação do disposto no n.º 2 do artigo 18.º, n.º 2 do artigo 26.º, e artigo 1.º, todos da CRP[219].

Por seu turno, JOÃO CONDE CORREIA também defendeu que o *malware* como meio de obtenção de prova já é hoje permitido, concretamente, pelo n.º 2 do artigo 19.º da LCc. Argumenta com o elemento gramatical, isto é, que as buscas *online* resultam da possibilidade de recorrer "*a meios e dispositivos informáticos*". Refere, contudo, que a letra da lei baliza a possibilidade de recurso a este meio, excluindo a possibilidade de uso no contexto das ações encobertas. Mas acaba por criticar o facto de não ser possível utilizá-lo nas expressões mais graves de criminalidade e questiona o catálogo de crimes em que é admitido este método[220].

FRANCISCO MARCOLINO DE JESUS também defende que o uso de *malware* está previsto na LCc, quando afirma que a "*Lei 109/2009, de 15/09, ao que se crê, permite a busca online*"[221]. Porém, não fundamenta esta sua crença. Acrescenta que "*caso se entenda que não tem suficiente densidade normativa, tal implica de acordo com Costa Andrade, que a busca on-line não possa ser realizada, seja em que circunstância for, por falta de um pressuposto cuja inexistência implicaria violação do princípio da legalidade*[222]".

Por último, referimos PAULO PINTO DE ALBUQUERQUE, como igual defensor da previsão do uso de *malware* na LCc. Considera que "*a busca online foi agora consagrada pelo novo artigo 15.º da Lei n.º 109/2009, de 15.9*", o qual prevê a possibilidade de uma pesquisa informática, por despacho da autoridade judiciária ou mesmo decisão do órgão de polícia criminal. Mais adianta que, a nova lei não coloca quaisquer restrições no que diz respeito aos conteúdos dos dados que podem ser pesquisados, como acontece na apreensão informática, nem exige que a pesquisa, quer seja ordenada pelo Ministério Público quer pelos órgãos de polícia criminal, seja validada pelo juiz. Conclui, todavia, que esta intrusão na privacidade da pessoa lesada é desproporcional, face aos n.ºs 1 e 2

---

[219] *Ibidem*, cit., p. 234.

[220] Cf. CORREIA, João Conde, *Prova digital: as leis que temos e a lei que devíamos ter* in *Revista do Ministério Público 139 Julho/Setembro 2014*. Lisboa: Coimbra Editora. ISSN 0870-6107. pp. 29-59. Apesar de o autor utilizar o conceito de buscas *online*, podemos concluir, face à seguinte descrição apresentada, que se refere ao conceito de *malware*: "*mediante várias técnicas informáticas à distância, via internet, aceder aos dados contidos num computador, observá-los, monitoriza-los, copiá-los sem o conhecimento e consentimento do visado. Tal como um hacker, também o Estado pode intrometer-se num computador alheio e verificar o que lá está"* cit., p. 42.

[221] Cf. JESUS, Francisco Marcolino de, *Os Meios de Obtenção da Prova em Processo Penal*. 2.ª Edição, Coimbra: Almedina, 2015. ISBN 978-972-40-5874-0. p. 246.

[222] *Ibidem*, cit. p. 246.

do artigo 26.º e n.º 4 do artigo 32.º da CRP, os quais reservam ao juiz os atos instrutórios que representem uma intrusão na privacidade[223].

5.2.2 Defensores da inexistência de norma habilitante.

Noutra perspetiva RITA CASTANHEIRA NEVES considera que na LCc não está consagrada a possibilidade de recurso ao *malware*. De acordo com as suas palavras, nem no artigo 15.º nem no artigo 16.º da LCc se verifica a possibilidade de se efetuarem buscas *online*, no sentido de poderem ser recolhidos dados informáticos sem conhecimento do visado. Por um lado, o n.º 1 do artigo 15.º faz referência à presença da autoridade judiciária na diligência, o que é incompatível com a natureza oculta do meio. Por outro, as formas de apreensão dos dados informáticos apelando aos critérios de adequação e da proporcionalidade das alíneas a) a d) do n.º 7 do artigo 16.º da LCc acaba por significar «[q]eu não são admitidas, mesmo nestes meandros, as buscas *online*, realizadas ocultamente, sem que o visado tome conhecimento da diligência, porque não previstos na lei e em respeito ao princípio da legalidade»[224].

No mesmo sentido PAULO DÁ MESQUITA[225] considera que não se pode confundir a utilização de *malware* com os regimes previstos nos artigos 15.º e 16.º da LCc, os quais se aplicam às pesquisas e apreensões informáticas que são, por força da CBCc, regras gerais de processo penal sobre busca e apreensão de prova electrónica (artigo 19.º da CBCc). Apesar da terminologia da LCc, continua a aplicar-se o n.º 1 do artigo 174.º do CPP, isto é, quando existirem indícios de que os dados informáticos relacionados com um crime ou que possam servir de prova estejam num determinado sistema informático, é ordenada uma busca informática. Já no que diz respeito às apreensões, os pressupostos continuam a ser os dos n.ºs 1 e 3 do artigo 178.º do CPP. Ou seja, são apreendidos os sistemas informáticos e os dados informáticos que tiverem servido ou fossem servir à prática de um crime. Ante o exposto, não existe espaço para a instalação e utilização de *software* malicioso.

[223] *Apud* (RAMALHO, 2017, p. 342).
[224] NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal, Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*. 1ª Edição. Coimbra: Coimbra Editora, 2011. ISBN 978-972-32-1942-5. pp. 272-273 e 284.
[225] Cf. (MESQUITA, 2010, pp. 114-116).

Por seu turno, acompanhando o raciocínio de MANUEL DA COSTA ANDRADE[226], também não se pode permitir o recurso ao *malware* (ditas "buscas *online*"), por força do artigo 18.º da LCc. Isto, porque a busca *online* não configura, pelo menos exclusivamente, uma invasão ou devassa de um ato de telecomunicação, não podendo, em consequência, estar abrangida por normas da lei processual relativas à interceção das telecomunicações[227]. Referindo-se aos métodos ocultos de investigação este autor acrescenta que "*representam uma intromissão nos processos de acção, interacção e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dela se apercebam*"[228].

5.3 Posição que sustento.

Antecipamos e revelamos desde já que a nossa posição encontra-se do lado daqueles que pugnam pela inexistência de norma habilitante.

Temos presente e acompanhamos as preocupações relativas decorrentes do recurso ao *malware* por parte dos OPC, no sentido que provoca danos sociais, principalmente se pensarmos no respetivo alcance, ou seja, a possibilidade de atingir um elevado número de pessoas (terceiros inocentes afetados), a enorme quantidade de informações que pode vir a ser recolhida e ainda a restrição direitos fundamentais[229] (será pois consoante a maior ou menor compressão e restrição destes direitos que o legislador terá que ter em conta aquando da previsão legal - ligado ao desenvolvimento da personalidade o direito à integridade e confidencialidade dos sistemas técnico informacionais, direito à autodeterminação informacional, direito à reserva da intimidade da vida privada e familiar, direito à palavra quando por exemplo à ativado o microfone, o direito à imagem quando é ativada a câmara, direito à inviolabilidade do domicílio, direito à inviolabilidade das telecomunicações e demais meios de comunicação) e processuais dos arguidos (O princípio *Nemo Tenetur Se Ipsum Accusare* - direito à não autoincriminação)[230].

---

[226] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado", a reforma do Código de Processo Penal, Observações críticas sobre uma Lei que podia e devia ter sido diferente.* Coimbra: Coimbra Editora, 2009. ISBN 978-972-32-1726-1. pp. 145-168.
[227] *Ibidem*, cit., p.160.
[228] *Ibidem*, cit. pp. 104-105.
[229] Não desenvolvemos os direitos fundamentais afetados que a doutrina identifica como o meio de obtenção de prova mais invasivo e restritivo de direitos fundamentais. Assim (RAMALHO, 2017, p.354). Também VACIAGO, Giuseppe, *Remote Forensics and Cloud Computing: An Italian and European Legal Overview*, *Digital Evidence and Electronic Signature Law Review*, Vol. 8, 2011, p. 126, disponível na internet:<URL:https://journals.sas.ac.uk/deeslr/article/view/1961/1898>. [Consultado em 25/04/2025].
[230] Cf. CAMPOS, Juliana Filipa Sousa, *O Malware como Meio de Obtenção…*, cit., pp. 55-74.

No conflito existente entre a descoberta da verdade material e realização da justiça, não descuramos e desvalorizamos que quando se introduz um método de obtenção de prova como o *malware* tem-se em vista a descoberta da verdade material entendida como «busca da verdade material é, no processo penal, um dever ético e jurídico, mas o Estado, como titular que é do *ius puniendi*, também está interessado em que só os culpados de actos criminosos sejam punidos (*satius esse nocetem absolvi innocentem damnari*). É quase um lugar-comum dizer-se que a verdade material não pode conseguir-se a qualquer preço: há limites decorrentes do respeito pela integridade moral e física das pessoas; há limites impostos pela inviolabilidade da vida privada, do domicílio, da correspondência e das telecomunicações, que só nas condições previstas na lei podem ser transpostos. Componente essencial do princípio do Estado de Direito é a ideia de justiça, a qual exige também a manutenção de uma administração de justiça capaz de funcionar, devendo reconhecer-se as necessidades irrenunciáveis de uma acção penal eficaz e acentuar-se o interesse público numa investigação da verdade, o mais completa possível, no processo penal, sendo o esclarecimento dos crimes graves tarefa essencial de uma comunidade orientada pelo aludido princípio» ”[231].

Como verificámos, a utilização deste tipo de *software* (que a doutrina se refere como *malware*, *trojan*, cavalos de tróia) pode ter propósitos diferentes e consistir em métodos de recolha de informação distintos. A questão terminológica é, inclusivamente, discutida na UE e foi nesse sentido que em março de 2017 foi entregue o relatório *Legal Framewoks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*[232] à Comissão de Liberdades Civis, Justiça e Assuntos Internos que o havia solicitado. Em termos sucintos, este estudo (que incidiu sobre 6 países da EU e 3 extra comunidade europeia), concluiu que os países que já implementaram estas medidas possuem um conjunto de medidas que visam garantir que a utilização de técnicas de *hacking* seja proporcional e necessário[233].

[231] Assim, Ac. do TRL, de 8/05/2018, Processo 40/18.3JAPDL-5 (Relator:Cid Geraldo), disponível na internet:<URL:https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1f3c9b0655ae2b3f802582b00053b463?OpenDocument>. [Consultado em 25/04/2025].
[232] GUTHEIL, Mirja, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, Disponível na internet:<URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>. [Consultado em 08/05/2025].
[233] (RAMOS, 2022, p. 210).

Analisemos, pois, a possibilidade de utilização de *malware* por força dos artigos 15.º, 16.º, 18.º e 19.º, todos da LCc, invocados pelos autores como legitimadores da sua utilização.

Antes disso, vejamos que a LCc visou não só a introdução de novos meios de obtenção de prova, mas também adaptar os já existentes ao mundo digital, motivo pelo qual entendemos, desde já, pelo afastamento do *malware* do artigo 174.º do CPP, na medida em que este foi pensado para buscas num determinado local físico (reservado e não livremente acessível ao público) com o escopo de atividade dirigida à descoberta de algo (corpóreo) escondido ou dissimulado (veja-se que a apreensão de correio eletrónico do artigo 17.º da LCc exige autorização judicial). Acresce ainda que nos termos do artigo 174.º, n.º 4 do CPP (prazo de validade do despacho que autoriza a busca) e 177.º, n.ºs 1 e 2 do CPP (delimita o período temporal em que pode ocorrer buscas domiciliárias), as buscas domiciliárias, que comportam um grau de devassa e intrusão assinaláveis, exigem de igual forma intervenção judicial. Ora, ainda que seja percetível uma tentativa de aproximação entre o *malware* (principalmente quando é empregue o termo busca *online*) e a tradicional busca clássica, pelos motivos expostos, consideramos que as últimas se reconduzem a buscas a lugares físicos ao passo que se estivermos a aferir a sua previsão no que diz respeito à pesquisa e apreensão de dados informáticos teremos que centrar a nossa atenção nos artigos 15.º e 16.º da LCc. Tenha-se em conta que os dados informáticos não são corpóreos nem tangíveis (veja-se a este propósito o ponto 184 da minuta do relatório explicativo da Convenção Cibercrime relativamente ao artigo 19.º)[234].

Vejamos assim o artigo 15.º da LCc. Nesta norma, conseguimos descortinar aspetos de aproximação entre as pesquisas de dados informáticos e a utilização de *malware*. Ambos visam a recolha de elementos de prova, tendo em vista a descoberta da verdade, através da obtenção de dados que se encontram em sistemas informáticos reservados ou não livremente acessíveis ao público. O acesso pode ocorrer nos dois casos, presencialmente (*i.e.*, quando o acesso físico ao sistema informático visado surge na sequência de uma busca, revista ou quando for voluntariamente consentida por quem tiver o controlo dos dados – artigo 15.º, n.º 1 e n.º 3 da LCc) ou remotamente (através da *Internet* ou rede local – nos termos do artigo 15.º, n.º 5 da LCc). Como já tivemos oportunidade de explicitar, a extensão da pesquisa informática tem suscitado problemas

[234] Na parte que refere *"[…] os dados informatizados armazenados, por si só, não será considerados como algo tangível, pelo que não poderão ser adquiridos a título de investigações criminais e acções penais da mesma forma que os bens corpóreos […]*".

de admissibilidade quando os dados informáticos se encontram armazenados num sistema informático situado fora do território português. Relembramos que da CBCc decorre a restrição territorial do exercício de medidas processuais que ali se encontram previstas, *i.e.*, todos os artigos aplica-se apenas a medidas empreendidas a nível nacional (cf. Ponto 192 a Minuta do Relatório Explicativo da CBCc) A intenção, foi estabelecer a cooperação internacional como regra de investigação, quando os dados informáticos se encontram armazenados em servidores situados no estrangeiro, ressalvados os casos previstos no artigo 32.º da CBCc. Não obstante, há doutrina que refere que a pesquisa do artigo 15.º, n.º 1 da LCc também pode ser efetuada remotamente, ou seja, o acesso poderia ser efetuado via *online*[235] caso consista num único acesso (*Daten-Spiegelung*), por contraposição a acessos que decorram de forma contínua ou prolongada no tempo (*Daten-Monitoring)*. Neste caso, entende DUARTE NUNES que a lei ao não exigir que a pesquisa (porquanto se refere apenas à obtenção e não ao modo concreto da sua obtenção) apenas possa ser "*presencial*", "*física*", permite a busca *online* com base nesta modalidade. Não obstante o autor ainda avança razões, que em abstrato, seriam equacionáveis para concluir que a nossa lei não admite buscas *online*: necessidade da presença da autoridade judiciária durante a pesquisa informática (artigo 15º, n.º 1 LCc – regra que considera de cariz procedimental que a lei refere "*sempre que for possível*" pelo que a ausência não obsta à sua admissibilidade), a remissão para as regras de execução das buscas previstas no CCP e no Estatuto do Jornalista (artigo 15.º, n.º 6 da LCc) para dizer que o preceito não exige que a busca informática seja "*presencial*" nem ser limitada à apreensão de coisas corpóreas, as formas de efetivação da apreensão dos dados previstas no artigo 16.º, n.º 7, alíneas a) a d) e o facto da lei não impor a apreensão no local onde está o sistema informático podendo esta ocorrer à distância (aliás o artigo 15.º, n.º 5 prevê a apreensão *online*), tudo para sustentar a admissão das buscas *online*, concluindo "*E, por todas estas razões, entendemos que a busca online é admissível entre nós, à luz do art.º 15.º da Lei n.º 1009/2009*"[236]. Contudo, apesar de admitir que a lei não faz distinção entre estes tipo de acessos (único ou continuado), assinala que sendo a busca mais intensa nos casos em que a busca ocorre de forma contínua e prolongada no tempo (*Daten-Monitoring*) do que aquela que ocorre através de um único acesso, na medida em que encerra um grau de danosidade muito similar ao grau de danosidade da interceção de comunicações, ainda

[235] Cf. NUNES, Duarte Alberto Rodrigues, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*. 1ª Edição. Coimbra: Gestlegal, 2018. ISBN 978-989-54076-4-4. p.231.
[236] *Ibidem*, cit., p. 231.

que a norma habilitante seja a o artigo 15.º da LCc, haverá que levar a cabo uma interpretação conforme à CRP e, por isso, a busca *online* na modalidade *Daten-Monitoring* deverá reger-se pelo disposto no artigo 18.º da LCc[237].

Ora, o artigo 15.º, n.º 5 da LCc, inspirando-se como já referimos no regime das buscas previsto no artigo 174.º do CPP (presenciais em espaços físicos), pelas razões supra expostas, concluímos pela exclusão da sua aplicação.

Outro aspeto que aproxima a pesquisa de dados informáticos e o *malware* é a circunstância de ambos poderem surgir como métodos ocultos de investigação. Analisando, constatamos que, em regra, a realização da pesquisa informática está dependente da autorização prévia ou ordem por despacho da AJ com um prazo máximo de validade de trinta dias (artigo 15.º, n.º 1, n.º 2 e n.º 5 *in fine*). Esta formalidade (a par da que ocorre com a busca tradicional em espaço físico) visa assegurar que o visado tem de alguma forma conhecimento da realização da diligência, permitindo o controlo do cumprimento da legalidade. Na pesquisa informática, caso seja esse o propósito, cumprindo-se esta formalidade de entrega da cópia do despacho a quem "*tenha a disponibilidade ou controlo dos dados"* (artigo 176.º, n.º 1 CPP *ex vi* artigo 15.º, n.º 6 da LCc) será colocada em causa e comprometido o caráter oculto da medida. Se tivermos em consideração o exposto no artigo 15.º, n.º 3 da LCc encontramos situações nas quais os OPC podem aceder à pesquisa sem prévia autorização da autoridade judiciária[238]. A este respeito, diremos desde já que discordamos dos autores que consideram que a pesquisa deverá sempre ocorrer com o conhecimento do visado[239].

---

[237] (NUNES, 2019, p. 812).

[238] Releva que o regime previsto neste artigo é criticável quando comparado com o regime das buscas do CPP, nomeadamente com o que se encontra previsto no artigo 174.º, n.º 5, alínea b) do CPP. Em ambos se prevê a possibilidade das buscas e pesquisas, respetivamente, serem efetuadas por OPC sem prévia autorização ou ordem por despacho da autoridade judiciária competente. A distinção entre elas decorre do facto das pesquisas na LCc dependerem do consentimento de quem tiver a disponibilidade ou controlo dados, ao passo que nas buscas depende do consentimento dos visados e não por quem tiver a mera disponibilidade do local. Deste modo, a lei admite que a pesquisa possa ser efetuada por OPC, sem despacho prévio da parte da autoridade judiciária competente, e sem o consentimento do visado pela medida. Em sentido crítico sobre este aspeto, GAMA, António, LATAS, António, CORREIA, João [*et. al.*], *Comentário ao art.º 174.º* in *Comentário Judiciário do Código de Processo Penal – Tomo II – Artigos 124.º a 190.º.* 2.ª Edição. Coimbra: Almedina, 2020. ISBN 978-972-40-8209-7. p.580. Em §8 enfatiza-se "*Só o titular do direito constitucional afetado pode acordar na sua restrição. Quem não é titular do interesse jurídico protegido pela norma não tem capacidade para consentir na sua violação*".

[239] Cf. REAL, Rui Miguel dos Santos, *Apreensão, exame ou perícia e utilização processual de meios de prova existentes em material informático. Enquadramento jurídico, prática e gestão processual* In *Meios de obtenção de prova e medidas cautelares e de polícia*, Lisboa: CEJ, 2019, pp. 149-150, disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cej.justica.gov.pt/LinkClick.aspx?fileticket=Y-MYpPvoBeE%3d&portalid=30>. [Consultado em 25/04/2025].

Um último aspeto de aproximação entre as pesquisas de dados informáticos e o *malware* é o grau de devassa e intromissão que lhe é intrínseco. A este respeito recordamos PAULO PINTO DE ALBUQUERQUE quando refere que "*A busca online foi agora consagrada pelo novo artigo 15.º da Lei n.º 109/2009, de 15.9, que prevê a "pesquisa em sistema informático", por despacho da autoridade judiciária ou mesmo decisão do órgão de policia criminal. A lei não coloca quaisquer restrições relativamente aos conteúdos dos dados que podem ser pesquisados, ao invés do que sucede com a apreensão de dados informáticos. […]. Esta intrusão na privacidade da pessoa visada é manifestamente desproporcional, em face do artigo 26.º, n.º 1 e 2, e do 32.º, n.º 4, da CRP, que reservam ao juiz os actos instrutórios que representem uma intrusão na privacidade. Assim o artigo 15.º da Lei n.º 109/2009, seria inconstitucional, na medida em que permite que o MP e o OPC ordenem a pesquisa de um sistema informático, incluindo dados informáticos íntimos ou privados, sem o controlo prévio ou posterior da pesquisa por um juiz [...]*"[240].

Apesar da existência de alguns pontos de aproximação, a verdade é que o *malware* e as pesquisas informáticas assumem diferenças que justificam o afastamento do primeiro do enquadramento previsto no artigo 15.º da LCc. Por um lado as pesquisas informáticas logram a obtenção de dados informáticos "*específicos e determinados*", os quais dificilmente se conseguirão filtrar através da utilização do *malware*, não só pela circunstância de se poder aceder aos dados armazenados no sistema informático como também a outros que ali não se encontram armazenados mas que com aquele estejam interligados, bem como aqueles que venham a ser produzidos em tempo real. O afastamento também é percetível na medida em que na extensão da pesquisa de dados informáticos apenas é possível o acesso remoto aos dados informáticos armazenados num sistema informático ou numa parte diferente do sistema pesquisado acessível a partir do sistema inicial, ao passo que com o *malware* se acede indistintamente ao sistema informático pretendido e a outros com ele conectado. A questão suscitada relativa ao eventual comprometimento, quando tal se justifique, do caráter oculto da pesquisa informática quando se acede ao sistema inicial, não se coloca com o *malware* porque neste o acesso pode vir a ser indiferenciado sem que com isso se comprometa a natureza oculta. Acrescentamos ainda o facto, como vimos, que o *malware* pode comportar um leque extenso de funcionalidades, tornando o nível da devassa (em comparação com a

[240] ALBUQUERQUE, Paulo Pinto, *Comentário ao art.º 177.º*, in *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção dos Direitos Humanos*, 4.ª Ed. Atualizada, Lisboa: Universidade Católica Editora, 2011. ISBN 978-972-54-0295-5. p. 502.

pesquisa) muito superior. Neste sentido, concluímos que o *malware* não será enquadrável no artigo 15.º da LCc.

Após a pesquisa ou outro acesso legítimo, invariavelmente, segue-se a apreensão. Contrariamente ao artigo 19.º da CCiber, o artigo 16.º e artigo 17.º, ambos da LCc distingue entre apreensão de dados informáticos e apreensão de correio electrónico e registos de comunicações de natureza semelhante num sistema informático. Depreende-se, relativamente à apreensão de dados informáticos, que esta surge como um ato complementar à pesquisa e a sua efetivação carece de despacho de autorização da AJ competente, com a exceção prevista no artigo 16.º, n.º 2 (sem previa autorização por parte dos OPC quando haja urgência ou perigo na demora) e especificidades nas apreensões do artigo 16.º, n.º 3 (dados pessoais ou íntimos que são apresentados encapsulados ao juiz que avaliará a pertinência e relevância da sua junção aos autos). Ora, o *malware* também comporta a necessidade de verificação destes atos complementares, uma vez que após a sua instalação, segue-se o envio de dados para o OPC encarregue da investigação ou AJ competente, que que leva a supor a sua apreensão. Acontece que a apreensão de dados informáticos surge na LCc na sequência de uma pesquisa informática, que é distinta, como tentámos elucidar, da utilização de *malware*. Por conseguinte, a apreensão mediante recurso a este último não poderá justificar-se com o artigo 16.º da LCc. A respeito da integração dos métodos ocultos no âmbito deste preceito, diremos que a apreensão pode não apresentar uma natureza oculta, existindo divergência doutrinária, em que por um lado temos os que argumentam em sentido positivo DAVID SILVA RAMALHO[241]com fundamento de que "*quando seja necessário apreender prova armazenada num específico sistema informático, sem que o seu utilizador se aperceba, o recurso à extensão da pesquisa prevista no artigo 15.º, n.º 5, da Lei do Cibercrime estará automaticamente excluído, uma vez que esta consubstancia uma extensão da pesquisa no sistema informático inicial ao sistema informático acessível remotamente. Como tal, a pesquisa remota é uma medida desprovida de qualquer secretismo (excepto no caso improvável em que o investigador tenha acesso físico ao sistema informático do suspeito e este não o saiba), podendo inclusivamente ser presenciada pelo titular dos dados (cf. Artigo 176.º, n.º 1, do CPP ex vi artigo 15.º, n.º 6, da Lei do Cibercrime* " e em sentido contrário MARIA

[241] (RAMALHO, 2017, p. 133).

BEATRIZ SEABRA DE BRITO[242] com o fundamento de " *Entendemos que o art.º 16.º da Lei do Cibercrime se limita a elencar as formas legalmente autorizadas de apreensão de dados informáticos, mas nelas não incluindo a possibilidade de acesso remoto sem conhecimento do visado*".

A nossa posição a este respeito pende para o afastamento da sua integração do regime das apreensões, na medida em que já tivemos oportunidade de constatar que a utilização do *malware* acarreta a compressão e restrição de direitos fundamentais que justificaria, *de per si*, um preceito autónomo.

Vejamos agora o artigo 18.º da LCc no qual se admite a interceção de comunicações. Entre as várias características e formas de atuação do *malware*, vimos que este pode possibilitar a obtenção de dados em tempo real[243], pelo que poderíamos estar tentados a enquadrá-lo neste artigo. Vejamos, não devemos confundir a vigilância (que torna possível assistir a toda a atividade do sistema informático visado) que alguns *malware* induzem nos sistemas por si "infetados" com a interceção de e registo de transmissões de dados informáticos efetuado nos termos do artigo 187.º do CPP, *ex vi* artigo 18.º, n.º 4 da LCc. Este último preceito, contrariamente ao *malware*, exclui a recolha por via remota e oculta de dados armazenados e não armazenados no sistema informático, apenas permitindo "registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego". A atuação do *malware* nem sequer necessita que exista uma efetiva comunicação, uma vez que é mais abrangente que uma interceção, abrangendo a monitorização de toda a atividade desenvolvida pelo sistema informático visado, permitindo a recolha de dados armazenados e dados produzidos em tempo real. Este motivo, aliado aos anteriormente expostos, leva-nos a concluir que o *malware*, apesar desta vertente de monitorização e vigilância, apto a intercetar o registo de transmissões de dados informáticos, na verdade, não se confunde com a interceção de comunicações. É certo que a sua utilização por parte dos OPC se traduz, invariavelmente, numa ingerência em meios de comunicação (que podem ou não existir de acordo com o utilizador do sistema informático visado), motivo pelo qual nos termos do artigo 34.º, n.º 4 da CRP e do artigo 126.º, n.º 3 do CPP, consideramos este meios de obtenção de prova uma intromissão ou ingerência nas telecomunicações, pelo que legitimar a sua utilização

[242] BRITO, Maria Beatriz Seabra de, *Novas Tecnologias e Legalidade da Prova em Processo Penal, Natureza e enquadramento do GPS como método de obtenção de prova*, (Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto Coordenação). Coimbra: Almedina, 2018. ISBN 978-972-40-7640-9. p. 97.

[243] Cf. Ponto 208 do Relatório Explicativo da CCiber que a propósito das comunicações refere que a expressão "em tempo real" significa que a recolha de dados tem lugar aquando da transmissão.

por recurso ao artigo 18.º da LCc traduzir-se-ia numa inconstitucionalidade material por violação do artigo 18.º, n.º 2 e artigo 34.º, n.º 4, ambos da CRP.

Resta a análise do artigo 19.º da LCc, a denominada "acção encoberta em ambiente digital"[244] e verificarmos se a utilização do *malware* se poderá justificar e legitimar através deste artigo. Podemos desde já referir a partilha de uma característica com o *malware*, que veremos poderá vir a ser relevante, que é o facto de também ela possibilitar a recolha de dados armazenados e produzidos em tempo real.

Vimos, quando abordamos a figura do "agente encoberto informático" que inexiste no nosso ordenamento jurídico uma regulação expressa desta figura. A este respeito também vimos considerações acerca do AE, infiltrado e homem de confiança, referindo, que esta última é entendida, na doutrina e na jurisprudência, como um conceito extensivo que "*abrange todas as testemunhas que colaboram com as instâncias formais de perseguição penal, tendo como contrapartida a promessa de confidencialidade da sua identidade e actividade*"[245]. Neste sentido, apenas seriam admissíveis os agentes encobertos ou infiltrados e já não os provocadores. Constatamos também que a atuação destes agentes seria limitada, ou seja, estaria confinada à recolha de informações, estando impedidos de induzirem ou provocarem eles próprios a prática do crime, afastando as actividades provocadoras que estes pudessem vir em ter em ambiente digital (*v.g.* o envio do *malware* através de *hyperlinks* com conteúdo aparentemente ilícito com o propósito de revelar o endereço de IP do destinatário). Também aludimos ao facto destas ações realizarem-se no plano digital, atendendo ao catálogo de crimes da Lei n.º 101/2001, de 25 agosto e no artigo 19.º, n.º1 e n.º 2 da LCc. Neste âmbito, além da característica comum assinalada (recolha de dados armazenados e produzidos em tempo real), também verificamos que as "ações encobertas em ambiente digital" se aproximam do *malware*, devido à necessidade de "ocultação" da atividade desenvolvida pelos OPC. Temos por um lado a ocultação da qualidade do agente nas AcE e por outro lado a dissimulação e ocultação da instalação do *malware* no sistema informático visado.

Todavia, o *malware* e as AcE em ambiente digital não se confundem, desde logo atendendo à sua natureza, ou seja, o primeiro é um *software* que é instalado e recolhe, preferencialmente, prova de forma oculta para o visado, ao passo que nas segundas se

[244] (RAMALHO, 2017, p.283).
[245] SOUSA, Susana Aires de, *Agent provocateur e Meios Enganosos de Prova. Algumas Reflexões* in ANDRADE, Manuel da Costa, COSTA, José Faria, RODRIGUES, Anabela Miranda, ANTUNES, Maria João (Organização), *Liber Discipulorum para Jorge de Figueiredo Dias*. Coimbra: Coimbra Editora, 2003. ISBN 972-32-1193-9. p. 1222.

está perante funcionários de investigação criminal ou terceiros, que em virtude da confiança estabelecida com o suspeito, obtêm informações, planos e confidências[246]. Em suma, a figura do AE tem como aspeto típico, para além do sigilo da atuação, a procura de uma relação de confiança com o visado. Esta última não se encontra no *malware*, cuja introdução no sistema informático poderá ocorrer de diversas formas, a maior parte sem contactos ou interações diretas entre o OPC e o visado.

No entanto, poderemos questionar se o *malware* não poderá ser usado, de forma complementar, no âmbito de uma ação encoberta em ambiente digital. É partindo desta premissa, que alguma doutrina defende o enquadramento do *malware* no artigo 19.º, n.º 2 da LCc, com fundamento e suporte no elemento literal do preceito quando ali se refere ao "recurso a meios e dispositivos informáticos". A argumentação vai no sentido de que caso fosse intenção do legislador referir outros meios de prova já previstos na legislação, tê-lo-ia dito expressamente ou remetido de forma integral para os mesmos[247]. Ademais, reforçam este entendimento devido ao preceito consagrar uma remissão para o regime da interceção de comunicações "naquilo que for aplicável", o que pretende evidenciar que esses "meios e dispositivos informáticos", não coincidem com aquela[248]. Realçam que a inserção destes "meios e dispositivos informáticos" no regime das ações encobertas no ambiente digital transparece que os mesmos são, tal como aquelas, um meio (oculto) particularmente gravoso de investigação[249], o que é uma característica do *malware*. Por fim, destacam ainda a terminologia adotada na legislação de outros ordenamentos jurídicos relativa à consagração do malware[250], a qual surge, em certa medida, próxima da que está presente no artigo 19.º, n.º 2 da LCc.

Reconhecendo mérito e delas retirando ensinamentos, ainda assim temos alguma dificuldade em acompanhar esta doutrina. Fizemos questão de enunciar preceitos e conceitos técnicos que são tidos em conta em diversos diplomas e *guidelines* relativamente à prova digital, sistemas, equipamentos informáticos e eletrónicos. A expressão que consta deste artigo 19.º, n.º 2 da LCc, "meios e dispositivos informáticos"

[246] *Ibidem*, cit. p. 1223.
[247] (RAMALHO, 2017, p. 344).
[248] *Ibidem*, cit., p. 343.
[249] *Ibidem*, cit., p. 344.
[250] *Ibidem*, cit., p. 346.

não é precisa e determinada, pelo que não se consegue recortar o seu âmbito com a segurança e certeza exigidas[251].

Assim, tendo em conta o caráter insidioso e invasivo do *malware*, os direitos fundamentais que são potencialmente restringidos, consideramos que só através de uma lei expressa, clara e determinada é que poderemos legitimar a sua utilização, acompanhando MANUEL DA COSTA ANDRADE, quando o mesmo partindo de considerações fixadas pelo Tribunal Constitucional Alemão no domínio das novas tecnologias, refere "Só uma lei expressa, clara e determinada, *especificamente reportada à técnica em causa*, definidora e delimitadora da respetiva medida de invasidade e devassa, pode legitimar a sua utilização como meio de obtenção de prova em processo penal"[252]. Assim, em conclusão, consideramos que o *malware* não pode ser legitimado ao abrigo do artigo 19.º, n.º 2 da LCc.

Referimos, ainda que em termos sucintos, a possibilidade de através do *malware* os OPC conseguirem, entre outros, ativar a câmara e microfone (*hardware*) do computador visado, recolhendo informações (imagem e som) que acabam por ser externas ao próprio sistema informático. Existem dois meios de obtenção de prova no nosso ordenamento que permitem a recolha de informação externa ao equipamento informático, referimo-nos à "interceção de comunicações entre presentes" (artigo 189.º, n.º 1, *in fine* do CPP) e a recolha de voz e imagem em tempo real (artigo 6.º, n.º 1 da Lei 5/2002, de 11 de janeiro)[253] sem conhecimento do visado. No entanto, «[…] tal registo apenas terá lugar para os crimes de catálogo mencionados no art.º 1.º, n.º 1, desta mesma lei, não existindo qualquer referência para o regime jurídico das ações encobertas»[254].

Consideramos que a utilização do *malware* como meio de obtenção de prova em processo penal justifica-se se for utilizada com o intuito de lograr a obtenção de prova digital encriptada em sistemas informáticos, cuja obtenção por parte dos OPC se mostre dificultada ou mesmo impossibilitada de obter, nos casos em que estejamos perante fenómenos criminais de maior gravidade (v.g. crime organizado em geral, terrorismo e crimes contra a vida).

---

[251] Alguma doutrina enquadra neste preceito diversos meios: a interceção de comunicações para fins de prevenção, os meios de obtenção de prova análogos à interceção de comunicações ou inclusivamente o *malware*. Dando-nos conta deste aspecto (RAMALHO, 2013, pp. 196-197).
[252] (ANDRADE, 2009, pp. 22-23).
[253] Disponível na internet:<URL: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=147&tabela=leis>. [Consultada em 28/04/2025].
[254] *Apud* (Ramos, 2022, pp. 218-219).

É certo que a sua utilização, como referimos, ocasionará a compressão e restrição de direitos fundamentais de arguidos, vítimas e terceiros envolvidos, no entanto, uma ponderação dos crimes em causa e da (in)existência de outros meios aptos a obter e recolher a prova digital (proporcionalidade), poderá justificar em meu entender a sua utilização, desde que exista legitimação legal, que como vimos, entendemos não estar verificada.

Conclusões

Os desafios que o contexto tecnológico impõe relativamente à recolha de prova digital transfronteiriça, suscita inúmeros problemas, um dos quais os conflitos de jurisdição. A prova digital pode estar armazenada em múltiplas jurisdições e devido à sua volatilidade importa criar mecanismos de cooperação ágeis e comunicantes, por forma a obter no âmbito das investigações a divulgação desses dados de forma eficaz e eficiente. Sem olvidar questões relacionadas com soberania e jurisdição dos Estados, não obstante a verificação de esforços e iniciativas para superar conflitos jurisdicionais, a verdade é que apesar da existência de instrumentos legais internacionais que representam passos significativos na tentativa de resolução de questões relacionadas com conflitos de jurisdição, a verdade é que eles ainda estão distantes, sendo que a própria UE ainda não dispõe de um sistema que atribua, de forma vinculativa, competências criminais nem tão pouco de um mecanismo vinculativo de resolução destes conflitos.

Urge corrigir esta situação e para esse desiderato, consideramos relevante a proposta de Directiva do ELI bem como deveras importante a implementação do *e-Evidence Digital Exchange System (e-EDES)*.

Por outro lado o atual contexto tecnológico impõe no âmbito da investigação da cibercriminalidade, a utilização de métodos ocultos de investigação, nomeadamente o *malware*. Tendo em conta o seu caráter insidioso e invasivo, os direitos fundamentais que são potencialmente restringidos, consideramos que só através de uma lei expressa, clara e determinada, que entendemos inexistir no nosso ordenamento jurídico, é que podíamos legitimar a sua utilização.

Neste sentido será nos termos supra expostos e com o devido enquadramento legal, por ora inexistente, que vislumbramos a utilização do *malware* como meio de obtenção de prova em processo penal.

Bibliografia

ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*. 2ª Edição atualizada. Lisboa: Universidade Católica Editora, 2008. ISBN 978-972-54-0197-2

ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*. 4ª Edição atualizada. Lisboa: Universidade Católica Editora, 2011. ISBN 978-972-54-0295-5

ALBUQUERQUE, Paulo Pinto, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção dos Direitos Humanos*. Volume I. 5.ª Edição atualizada. Lisboa: Universidade Católica Editora, 2023. ISBN 978-972-540-945-9

ALEXANDRINO, José Melo, *Lições de Direito Constitucional*. Volume I, 3ª Edição. Lisboa: AAFDL, 2017. ISBN 978-972-629-153-4

ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado", a reforma do Código de Processo Penal, Observações críticas sobre uma Lei que podia e devia ter sido diferente*. Coimbra: Coimbra Editora, 2009. ISBN 978-972-32-1726-1

ANTUNES, Margarida Neiva, *A Obtenção de Prova Digital Mediante Acessos Transfronteiriços em Contexto de Loss of Location* in *Novos Desafios da Prova Penal*, MENDES, Paulo Sousa / PEREIRA, Rui Soares (Coordenação), Vol.II. Coimbra: Almedina, 2023. ISBN 978-989-40-1059-3

BRITO, Maria Beatriz Seabra de, *Novas Tecnologias e Legalidade da Prova em Processo Penal, Natureza e enquadramento do GPS como método de obtenção de prova*, (Teresa Pizarro Beleza e Frederico de Lacerda da Costa Pinto Coordenação). Coimbra: Almedina, 2018. ISBN 978-972-40-7640-9

CAMPOS, Juliana Filipa Sousa, *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Almedina, 2021. ISBN 978-972-40-9021-4

CANOTILHO, José Gomes / MOREIRA, Vital, *Constituição da República Portuguesa Anotada* - (*Artigos 1.º a 107.º).* Volume I. 4.ª Edição. Coimbra: Coimbra Editora, 2007. ISBN 978-972-32-1462-8

CORREIA, João Conde, *Prova digital: as leis que temos e a lei que devíamos ter* in *Revista do Ministério Público 139 Julho/Setembro 2014*. Lisboa: Coimbra Editora. ISSN 0870-6107. pp. 29-59.

GAMA, António, LATAS, António, CORREIA, João [*et. al.*], *Comentário ao art.º 174.º* in *Comentário Judiciário do Código de Processo Penal – Tomo II – Artigos 124.º a 190.º*. 2.ª Edição. Coimbra: Almedina, 2020. ISBN 978-972-40-8209-7

JESUS, Francisco Marcolino de, *Os Meios de Obtenção da Prova em Processo Penal*. 2.ª Edição, Coimbra: Almedina, 2015. ISBN 978-972-40-5874-0

LEITE, Inês Ferreira, *O conflito de leis penais – Natureza e Função do Direito Penal Internacional*. Coimbra: Coimbra Editora, 2008. ISBN 978-972-32-1564-9

MARTÍN, Cristos Velasco San, *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*. Valencia: Tirant Lo Blanch. 2016. ISBN 978-84-9086-992-5

MENDES, Paulo Sousa, PEREIRA, Rui Soares (Coordenação), *Novos Desafios da Prova Penal*, Vol. II. Coimbra: Almedina, 2023. ISBN 978-989-40-1059-3

MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, 1ª Edição. Coimbra: Coimbra Editora, 2010. ISBN 978-972-32-1842-8

NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal, Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*. 1ª Edição. Coimbra: Coimbra Editora, 2011. ISBN 978-972-32-1942-5

NUNES, Duarte Alberto Rodrigues, Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime. 1ª Edição. Coimbra: Gestlegal, 2018. ISBN 978-989-54076-4-4

NUNES, Duarte Alberto Rodrigues, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal como Instrumento de Resposta à Criminalidade Organizada*.1ª Edição. Coimbra: Gestlegal, 2019. ISBN 978-989-8951-29-8

PANZAVOLTA, Michele, *Choosing the National Forum in Proceedings Conducted by the EPPO: Who Is to Decide?* in WINTER, Lorena Bachmaier, *The European Public Prosecutor's Office: The Challenges Ahead - Legal Studies in Internacional, European and Comparative Criminal Law 1*. Volume I. Cham, Switzerland: Springer Nature Switzerland AG, 2018 (pp.59-83).ISBN 978-3-319-93915-5

PEREIRA, Rui Soares, *Prova, Verdade e Processo*. Coimbra: Almedina, 2023. ISBN 978-989-40-1291-7

PRADILLO, Juan Carlos Ortiz, *"Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquência informática, Revista de Derecho y Proceso Penal*, n.º 26, ano 2011-2, Navarra: Editorial Aranzadi, 2011.

PUIGVERT, Sílvia Pereira / PONZ, Francesc Ordóñez (Directores) / ZAMORA, María Jesús Pesqueira (Coordinadora), *Investigación Y Processo Penal en el Siglo XXI Nuevas Tecnologías Y Protección de datos*, Editorial Arazandi, 2021. ISBN 978-84-1390-520-4

RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017. ISBN 978-972-40-7000-1

RAMOS, Armando Dias, *O Agente Encoberto Digital, Meios Especiais e Técnicos de Investigação Criminal*. Coimbra: Almedina, 2022. ISBN 978-989-40-0258-1

RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital.* Coimbra: Coimbra Editora, 2009. ISBN 978-989-95779-5-4

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente…, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. 1ª Edição. Rei dos Livros, 2010. ISBN 978-989-8305-06-0

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV, Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital.* 1ª Edição. Rei dos Livros, 2011. ISBN 978-989-8305-18-3

ROQUE, Miguel Prata, *A Dimensão Transnacional do Direito Administrativo – uma visão cosmopolita das situações jurídico-administrativas*. 1ª Edição. Lisboa: AAFDL, 2014. Depósito legal n.º 378111/14.

SOUSA, Susana Aires de, *Agent provocateur e Meios Enganosos de Prova. Algumas Reflexões* in ANDRADE, Manuel da Costa, COSTA, José Faria, RODRIGUES, Anabela Miranda, ANTUNES, Maria João (Organização), *Liber Discipulorum para Jorge de Figueiredo Dias*. 2003. Coimbra: Coimbra Editora. ISBN 972-32-1193-9

Consultados na Internet:

BARLOWEM, Bill *et al.*, *Microsoft Security Intelligence Report: Special Edition*, 2012. Disponível na Internet:<URL:https://download.microsoft.com/download/2/9/6/296f22f6-fd58-409e-adc8-6024d7fe3a35/Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review_Portuguese.pdf>.

BOLDT, Martin, *Privacy-Invasive Software*, Karlskrona: Blekinge Institute of Technology, 2010. ISBN 978-91-7295-177-8. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diva-portal.org/smash/get/diva2:835533/FULLTEXT01.pdf >.

GERCKE, Marco, *Understanding Cybercrime: phenomena, challenges and legal response*, 2012.
Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.itu.int/ITU-D/cyb/Cybersecurity/docs/cybercrime%20legislation%20EV6.pdf >.

GUTHEIL, Mirja *et. al.*, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices: Study for the LIBE Committee*, 2017.
Disponível na internet:<URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf >.

HARRIS, Ryan, *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Digital Investigation - The international Journal of Digital Forensics & Incident Response* [Em linha], Vol.3, 2006, pp. 44-49.
Disponível na internet: <URL:https://www.sciencedirect.com/science/article/pii/S1742287606000673>.

Koops, Bert-Jaap, *Police investigations in Internet open sources: Procedural-law Issues, 29 Computer Law & Security Review (6*), 2013, pp. 654-665.
Disponível na internet: <URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2574951>

OHM, PAUL, "*The Investigative Dynamics of the Use of Malware by Law Enforcement"*, *William & Mary Bill of Rights Jounal*, Vol. 26, n.º 2, 2017, pp. 303-334.
Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1836&context=wmborj>.

ORLANDO, Claudio, *Mutua Ammissibilità Della Prova Tra Gli Stati Membri DellÚnione Europea Ed E-Evidence: Riflessiooni a Margine Della Proposta Di Direttiva Dello European Law Institute* in *Sistema Penale (SP)*. 11/2023. ISSN 2704-8098.
Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sistemapenale.it/fascicoli/1701360858_fasc-112023.pdf>.

PAYER, Andrés, *El principio de territorialidade y la participación delictiva transnacional* in Revista Penal [Em linha]. N.º 53 (2024), pp. 203-222.

Disponível na internet:<URL:https://revistapenal.tirant.com/index.php/revista-penal/article/view/102/84>.

PFEFFERKORN, Riana, *Security Risks of Government Hacking*, *The Center of Internet and Society*, 2018.
Disponível na internet:
<URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cyberlaw.stanford.edu/content/files/sites/default/files/publication/files/2018.09.04_security_risks_of_government_hacking_whitepaper.pdf>.

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 na Internet:
<URL:http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf>.

REAL, Rui Miguel dos Santos, *Apreensão, exame ou perícia e utilização processual de meios de prova existentes em material informático. Enquadramento jurídico, prática e gestão processual* In *Meios de obtenção de prova e medidas cautelares e de polícia,* Lisboa: CEJ, 2019, pp. 149-150.
Disponível na internet:
<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cej.justica.gov.pt/LinkClick.aspx?fileticket=Y-MYpPvoBeE%3d&portalid=30>.

RAMALHO, David Silva, *O Uso de Malware Como Meio de Obtenção de Prova em Processo Penal* in Revista de Concorrência e Regulação [Em linha]. Ano IV, n.º 16 (2013), 195-243.
Disponível na Internet:
<URL:https://catalogo.pgr.pt/cgi-bin/koha/opac-detail.pl?biblionumber=243580>.

RAMALHO, David Silva, *A recolha de prova penal em sistemas de computação em nuvem* in *Revista de Direito Intelectual*, n.º 2 (Dez. 2014), pp. 123-162.
Disponível na internet:
<URL:https://catalogo.pgr.pt/cgi-bin/koha/opac-detail.pl?biblionumber=246778>.

RAMALHO, David Silva, *A investigação Criminal na Dark Web*. Revista de Concorrência e Regulação. Ano IV, Número 14/15 (2013), pp. 383-429).
Disponível na internet:

<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.concorrencia.pt/sites/default/files/imported-magazines/CR14_15_-_Victor_Castro_Rosa.pdf>.

SANTOS, Antonio Martínez, *Admisibilidad Mutua de Prueba Penal Transfronteiriza en La Unión Europea: La Propuesta de Directiva Del European Law Institute* in *Revista General de Derecho Procesal*, N.º 61. 2023. ISSN 1696-9642. Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Admissibility_of_E-Evidence/426388-1.pdf>.

SEITZ, Nicolai, *Transborder Search: A New Perspective in Law Enforcement, 7 Yale J.L. & Tech.23*, 2005.
Disponível na internet:
<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://yjolt.org/sites/default/files/seitz-7-yjolt-23.pdf >.

SIMMA, Bruno e MULLER,Andreas Th., *Exercise and limits of Jurisdiction, in The Cambridge Companion to International Law*, Edited by James Crawford and Martti Koskenniemi, Assistant Editor Surabhi Ranganathan, Cambridge University Press. [Em linha]. 2012, pp. 134-157.
Disponível na internet:
<URL:https://www.researchgate.net/profile/Andreas-Mueller-78/publication/321376192_Exercise_and_limits_of_jurisdiction/links/60f1ad0816f9f313008b453a/Exercise-and-limits-of-jurisdiction.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19>.

VACIAGO, Giuseppe, *Remote Forensics and Cloud Computing: An Italian and European Legal Overview, Digital Evidence and Electronic Signature Law Review*, Vol. 8, 2011.
Disponível na internet:<URL:https://journals.sas.ac.uk/deeslr/article/view/1961/1898>.

VERDELHO, Pedro, Pesquisa e Apreensão de dados com consentimento do titular, Nota Prática nº 29/2025 21 de abril de 2025.
Disponível na internet:
<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cibercrime.ministeriopublico.pt/sites/default/files/2025-04/nota-pratica-pesquisa-e-apreensao-de-dados-consentidas-2025.04.21.pdf>.

VERVAELE, John A.E., *European criminal justice in the post-Lisbon area of freedom, security and Justice.* Editorial Scientifica, Napoli. [Em linha]. (2014), pp. 1-312.
Disponível na internet:
<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://core.ac.uk/download/pdf/150084157.pdf>.

WINTER, Lorena Bachmaier, SALIMI, Farsam, RAMOS, Vânia Costa [Et. al], *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings – Draft Legislative Proposal of the European Law Institute*. Vienna: European Law Institute, 2023. ISBN 978-3-9505318-6-2.
Disponível na internet:<URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>.

Jurisprudência consultada

Acórdão do TRL, Proc. 6919/2003-5, Relator Ana Sebastião, de 15-06-2004:
Disponível na internet:
<URL:https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/460fbcb260b446bc80256fc0003d65e6?OpenDocument&Highlight=0,corrup%C3%A7%C3%A3o,c%C3%B3digo,penal>.

Acórdão da Terceira Secção do TEDH de 24 de junho de 2004, Von Hannover c. Alemanha, queixa n.º 59320/00:
Disponível na internet:
<URL:https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-61853%22]}>.

Acórdão da Quarta Secção do TEDH de 12 de janeiro de 2010, Guillan e Quinton c. Reino Unido, queixa n.º 4158/05:
Disponível na internet:
<URL:https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-96585%22]}>

Acórdão STJ, Proc. 127/10.0JABRG.G2.S1, Relator Santos Cabral, de 27/06/2012:
Disponível na internet:
<URL:https://juris.stj.pt/ecli/ECLI:PT:STJ:2012:127.10.0JABRG.G2.S1.9F?search=EeyHz_bdOz8AN0d86nI>.

Acórdão do STJ, Proc. 1/13.9YGLSB.S1, Relator Raul Borges, de 17/04/2015:
Disponível na internet:
<URL:https://juris.stj.pt/ecli/ECLI:PT:STJ:2015:1.13.9YGLSB.S1.01?search=PcIFmbZpy7b5oviavAU>.

Ac. TRP, Proc. 2039/14.0JAPRT.P1, Relator José Carreto, de 07-07-2016:
Disponível na internet:
<URL:https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cffe710b2cb8d91e8025800500475ea9?OpenDocument>.