UNIVERSIDADE
CATÓLICA
PORTUGUESA

Faculdade de Direito – Escola de Lisboa

Mestrado Forense

Buscas informáticas e subsequente apreensão de dados informáticos como métodos de obtenção de prova digital em Processo Penal:

Uma análise crítica do regime vigente e da mais recente perspetiva de evolução legislativa.

Dissertação de Mestrado orientada pelo

Senhor Professor Doutor Henrique Salinas

Mª Frederica dos Santos Queirós Rodrigues Colaço

31 de Março de 2023

“*To be left alone is the most precious thing one can ask of the modern world***.”**

— Anthony Burgess, Homage to Qwert Yuiop: Essays

Índice de conteúdos

PALAVRAS-CHAVE:

Prova digital; Buscas informáticas, Apreensões; dados informáticos; processo penal; cibercrime; direitos dos arguidos; regime atual; regime proposto; obtenção de prova; ambiente digital; competência; natureza das normas; correio eletrónico; palavra virtual; correio aberto; correio fechado;

SIGLAS E ABREVIATURAS

Ac. – Acórdão

APUD - citado por

Art.- artigo

Cf.- confira

CCiber. – Convenção do Cibercrime

CPP- Código do Processo Penal

CRP- Constituição da República Portuguesa

JIC- Juiz de Instrução Criminal

MP- Ministério Público

OPC- Órgãos de Polícia Criminal

TJUE- Tribunal de Justiça da União Europeia

I. Introdução

1. Contexto histórico-social – a Era Digital

Com mais de 80% da população portuguesa a passar em média 8 horas por dia no ciberespaço[1], parece impossível que uma outra realidade não se imiscua na aldeia global[2] da *internet.* O cibercrime, ou crime informático (adaptada da expressão inglesa *computer crime*) ou ainda crime tecnológico, na sua adaptação de *high tech crime*[3] é uma verdadeira consequência incontornável desta evolução tecnológica. «O ciberespaço, a sua espinha dorsal é, por definição, independente e anárquica, ingovernável e irreprimível. É a consequência da sua virtualidade: de estar em toda a parte e de não estar em lado nenhum. No ciberespaço, qualquer pessoa pode manifestar-se ou expressar-se, sem censura ou coação. Para o bem e para o mal.»[4] . Podemos afirmar, na senda de Benjamim Silva Rodrigues (2009), que o mundo digital vem sendo apropriado pelos criminosos que encontram novas oportunidades, até então desconhecidas. Diretamente proporcional à rápida adaptação criminosa aos novos meios, foi também o esforço legislativo de combate à mesma.[5]

2. A Prova Digital

Face a estas evoluções (tecnológicas e de criminalidade), o desafio que se impõe ao legislador é acompanhá-las de forma coerente, coesa e com foco nos princípios fundamentais que dirigem o processo penal, de forma a criar uma adequada defesa face à cibercriminalidade (e que não se torne obsoleta com qualquer avanço tecnológico) uma vez que, hoje em dia, estes avanços são diários e têm um efeito multiplicador avassalador.

---

[1] Palavra cunhada por William Gibson na sua obra de ficção científica *Neuromancer.*

[2] Conceito proposto por Marshall Mcluhan (1964) de uma aldeia global, falando de uma verdadeira aldeia virtual, cheia de "seres digitais".

[3] VERDELHO, 2003

[4] VERDELHO, 2003

[5] A este respeito leia-se a sintetização de Sieber (apud LOURENÇO MARTINS, 2003) quanto ao desenvolvimento da legislação no que toca à criminalidade informática.

Não é uma tarefa fácil. Relembramos os ensinamentos de Figueiredo Dias, que afirma que

> «(…) **o processo penal decorra por meios e por formas processualmente válidas, assumindo esta questão, como é evidente, primacial importância em matéria de prova**.»[6] [7]

A nível de matéria probatória, a prova digital impõe-se como um dos institutos mais complexos, especialmente tendo em conta a sua atualidade.

Acompanhamos Benjamim Silva Rodrigues (2009) no que diz respeito às dificuldades no combate à criminalidade informática, identificando três elementos: a «localização e identificação dos delinquentes» - implica o acesso e análise de dados criados pela pegada informática deixada pelos mesmos, que deverá sempre ser conciliado com os direitos fundamentais dos visados, nomeadamente no que toca à privacidade, autodeterminação comunicacional, entre outros direitos (que veremos a seu tempo) - a «preservação de elementos de prova» - que terá implicações quer a nível de recolha, bem como de tratamento dos dados recolhidos, sempre com respeito pelos direitos em causa; - e, por fim, o «lugar de armazenamento dos dados» - que terá a ver com a característica da globalidade supramencionada e o facto de os dados objeto de uma busca a um computador em Portugal poderem estar, na verdade, armazenados no estrangeiro.

Destes desafios focar-nos-emos nos primeiros dois, que se centram maioritariamente nos dois métodos de obtenção de prova que nos propomos a analisar neste âmbito: as buscas informáticas e as apreensões de dados informáticos.

Como veremos, estes métodos de obtenção de prova fazem parte de um regime probatório informático, ou digital, que se encontra espalhado por vários diplomas, sendo alvo de variadíssimas críticas e objeções, afigurando-se como um dos regimes mais controversos e que maior atenção merece nesta era digital. É um dos maiores desafios impostos ao direito processual penal: o de se manter relevante e eficaz no combate ao cibercrime, realidade em constate evolução, mutação e suscetível de tornar os mais adequados instrumentos obsoletos em pouco tempo. É necessário que exista um regime que seja

---

[6] Sublinhado nosso.

[7] FIGUEIREDO DIAS, 2017

adequado, eficaz, mas principalmente que possa prevalecer ao passar do tempo.. Cabe, da nossa parte, uma análise crítica do regime atual, e uma proposta ponderada para um regime que melhor servirá a causa, dando, por um lado, cumprimento aos objetivos de prossecução da verdade material e alcance da justiça do estado de direito, e por outro, a proteção dos princípios e direitos fundamentais garantísticos dos arguidos em processo penal, que se impõem de especial importância face a uma (já não tão) nova realidade que tanto potencial têm para violações dos mesmos.

3. Enquadramento da problemática à luz do artigo 5º do Decreto n.º 167/XIV e apreciação de constitucionalidade do mesmo pelo Tribunal Constitucional[8]

Como já foi mencionado e como será aprofundado mais adiante, os métodos de obtenção de prova digital constam de vários instrumentos. Nomeadamente, e central nesta matéria, a lei 109/2009, apelidada Lei do Cibercrime.

Em 2021 o Governo veio, no Decreto n.º 167/XIV, propor uma alteração ao artigo 17º da Lei do Cibercrime, (artigo que incide sobre a apreensão de correio eletrónico e registos de comunicação de natureza semelhante) que visava o seu esclarecimento. No entanto, a constitucionalidade desta alteração foi posta em causa, e o Tribunal Constitucional considerou *a final* que esta nova redação era, de facto, inconstitucional.

Assim, é importante a análise, paralela ao regime atual, desta proposta, e das suas fraquezas, para efeitos de ponderação de uma eventual evolução legislativa bem-sucedida.

O atual regime de buscas e apreensões constantes da Lei do Cibercrime é altamente controverso, gerando querelas doutrinais que a cada dia se acentuam, com a constante e exponencial evolução tecnológica a que assistimos à data. Por essa razão, para além de ser importante a análise do regime tal como é, e das dúvidas que se geram sobre o mesmo, é também fulcral perceber qual foi o rumo que esta tentativa legislativa tomou, quais foram as discussões doutrinais que se tentaram apaziguar, e acima de tudo, qual foi a decisão do Tribunal Constitucional sobre esse processo, revelando assim, qual é de momento, a posição do Tribunal quanto a certas querelas doutrinais importantes sobre o

[8] Acórdão do Tribunal Constitucional nº 687/2021

tema, tentando deste modo desbravar um caminho pelo qual se deva seguir no percurso evolutivo da prova digital.

Será, então, esta decisão que acompanhará este estudo, procurando sempre expor como o Tribunal Constitucional se debruçou sobre as temáticas abordadas aqui e quais as conclusões que foram sendo formadas.

Não parece descabido afirmar que nos depararemos com ideias que apoiam o nosso estudo, uma vez que já sabemos a decisão final de inconstitucionalidade sobre uma alteração que é coerente com as decisões que têm informado o exercício legislativo relativamente ao cibercrime e aquisição de prova digital.

II. Enquadramento legal

1. Plano internacional

1. Convenção sobre o Cibercrime, de 23 de novembro de 2001

Ao falar de cibercrime é incontornável começar pela Convenção do Conselho da Europa sobre a Cibercriminalidade[9], aberta à assinatura em novembro de 2001.

A convenção contém, entre outros, inovações a nível processual. A saber: a definição de preservação expedita de dados, medidas para a conservação célere de dados informáticos registados, revelação de dados de tráfego relativos a mensagens; injunções destinadas à divulgação de dados que estejam na posse de terceiros; interceção de conteúdos, e recolha de dados em tempo real; e por fim as normas relativas à busca informática e apreensões em ambiente digital.[10]

Uma breve análise da Convenção obriga menção a quatro normas importantes.

O artigo 14º consagra o âmbito de aplicação das medidas processuais plasmadas na Convenção aos crimes por ela definidos. No entanto, este artigo contempla duas extensões bastante relevantes. Por um lado, a extensão a qualquer outro tipo de crime cometido por via de sistema de computadores; e por outro lado, à obtenção de prova em forma eletrónica no que toca a ilícitos penais. Estas extensões são de particular importância na

[9] Doravante: CCiber

[10] LOURENÇO MARTINS, 2003; VERDELHO, 2003

medida em que foram adotadas por Portugal, em pleno, na Lei 109/2009, com várias implicações. Remetemos aqui para o subcapítulo relativo à Lei do Cibercrime.

Os artigos 16º e 17º da Convenção que preveem a preservação expedita e revelação de dados armazenados num computador, e a preservação expedita e revelação de dados de tráfego. «A previsão destas duas medidas processuais é separada. Tal separação é motivada pelo diferente enfoque de ambas».[11] Ainda que ambas sejam medidas expeditas impostas pela velocidade de circulação da informação no ciber ambiente, que ambas sejam inovadoras e essenciais para o sucesso de investigações criminais no plano digital, a realidade é que, por outro lado, são medidas diferentes. Em relação aos dados de tráfego está prevista a sua revelação expedita, tal já não ocorre quanto aos dados de comunicação, ou dados já armazenados, relativamente aos quais se pugna pela sua mera preservação até se obter pelas vias normais a ordem judicial para a sua obtenção material.

A nível de matéria de busca e apreensão de dados informáticos armazenados o artigo 19º parece fazer coincidir as medidas expostas, com as tradicionais formas de busca e apreensão, pese embora, neste âmbito, aplicadas à realidade específica do ciberespaço. Trata-se da adaptação de dois métodos já conhecidos de obtenção de prova a uma realidade com particularidades que assim o exigem.

A novidade processual encontra-se plasmada no nº2 deste artigo, que prevê que no âmbito de uma busca a um sistema de computadores o investigador se depare com o facto de os dados objeto da busca se encontrarem armazenados num outro sistema de computadores, acessível através do primeiro, que se encontre em território nacional, poderá, expeditamente, estender a busca a esse outro sistema.

A inovação reside principalmente no facto de em regra, as entidades que executam a busca ordenada por entidade competente, não terem competência para, por si só, estenderem o âmbito da mesma[12]. Esta regra permite que os Órgãos de Polícia Criminal, por exemplo, ao executar uma busca a um computador determinado, possam aceder também a um outro localizado em qualquer outra parte do território, sem informar o titular desse outro computador, desde que seja acessível através do primeiro. Esta novidade também foi

[11]VERDELHO, 2003

[12] VERDELHO, 2003

integralmente adotada pelo legislador nacional, pelo que será analisada a fundo em sede própria.

Em relação às apreensões, está previsto que os Estados devem legislar no sentido de prever a mera apreensão de dados, e elaboração de uma cópia dos mesmos, mantendo a integridade dos mesmos.

2. A Decisão Quadro 2005/222/JAI do Conselho, de 24/02/2005

Breve referência deve ser feita, também, à Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005. Este instrumento de direito internacional público é relativo a ataques contra sistemas de informação, e «no essencial acompanha a Convenção sobre o Cibercrime» e «tem por objetivo a harmonização das legislações dos Estados membros, pese embora desta feita apenas relativamente à: — delimitação de conceitos jurídico-informáticos; — tipificação de crimes informáticos; — fixação de regras sobre a aplicação espacial da lei penal relativamente a estes crimes; — implementação de medidas de cooperação internacional com vista à obtenção de prova digital e, genericamente, ao combate à criminalidade informática».[13]

2. Plano nacional

A nível de direito nacional,

> «as peças do puzzle não se encaixam facilmente. (…) em vez de seguir o velho conselho iluminista e de optar por poucas leis simples e claras, o legislador escolheu a via incerta da pluralidade e da complexidade, gerando um sistema anárquico, onde, muitas vezes, nem a sua letra, nem o seu espírito, nem, tão pouco, a sua história fornecem a bússola necessária para encontrar o caminho mais seguro (…), a jurisprudência dificilmente conseguirá resolver a quadratura do círculo, ou desatar os apertados nós que o legislador (…) foi atando.»[14]

[13] LOPES MILITÃO, 2012

[14] CONDE CORREIA, 2014

1. Código de Processo Penal[15]

O Código de Processo Penal, é, por excelência, o instrumento que reúne, à partida, todas as matérias e disposições relevantes do direito processual penal. Nos artigos 174º a 186º vêm estabelecidos os regimes, respetivamente, das buscas e das apreensões como métodos de obtenção de prova.

João Conde Correia (2014) identifica que o primeiro "nó" atado pelo legislador se dá ao estender o regime de interceções telefónicas para outras realidades distintas, nomeadamente para outras conversas ou comunicações por qualquer outro meio diferente do telefone, mesmo que se encontrem guardadas em suporte digital (artigo189º, nº 1 CPP).

Acompanhamos João Conde Correia (2014) numa breve análise evolutiva deste preceito: em 1998 foi densificado, através da reforma concretizada pela Lei nº 59/98, alargando o regime "às conversações ou comunicações transmitidas por qualquer meio diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como à interceção das comunicações entre presentes.". Assim, resulta evidente que o legislador, mesmo à data, não ignorava o valor probatório do correio eletrónico. Em 2007, através da lei 48/2007, foi alterada a numeração daquele artigo (que passou a ser o atual 189º, nº 1 do CPP) e concretizados, novamente, os termos da equiparação acrescentando que o regime se estendia a "(…) outras formas de transmissão de dados por via telemática, *mesmo que se encontrem guardadas em suporte digital* (…)"

A «interpretação desta norma, já denominada 'casa dos horrores' hermenêuticos[16], não é simples nem linear»[17] criando, de facto, o primeiro, mas certamente não o último, nó na legislação nacional sobre a prova digital.

---

[15] Doravante CPP

[16] Expressão de Costa Andrade (2009)

[17] CONDE CORREIA, 2014

2. A Lei n.º 32/2008

A Lei nº32/2008 veio, por força de necessidade de transposição de obrigações internacionais – mais especificamente da Diretiva nº 2006/24/CE do Parlamento Europeu e do Conselho, de 15/03/2006, cujo prazo de transposição havia terminado em Setembro de 2007 – regular a conservação e transmissão de dados – de tráfego e de localização, bem como os conexos necessários para identificar o assinante ou utilizador registado - gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, pra fins de investigação e repressão de crimes graves.[18]

Este diploma veio agravar e densificar as dificuldades interpretativas sobre a recolha de prova digital, uma vez que uma coisa é a preservação de dados, e outra, diferente, mas sobre a qual este regime incide também, é a sua aquisição e valoração processual penal. A verdade é que «apesar de convocar requisitos de acesso semelhantes, o legislador, sem qualquer razão técnica válida, duplicou os regimes, consagrando normas gerais no Código de Processo Penal, e normas especiais na lei nº 32/2008.»[19]

Na mesma linha Rita Castanheira Neves (2011) entende que o legislador «foi remediando à medida que compulsivamente tinha que publicar», uma vez que

> «na verdade, a ensaiar a Reforma de 2007, o legislador processual penal já estava na posse do que era necessário para ter reformulado o já mencionado Título dos Meios de Obtenção de Prova, autonomizando as soluções adequadas para os dados, não só de tráfego (e localização), como de conteúdo, apurados através de comunicações eletrónicas. Ter-se-ia, se assim tivesse ocorrido, evitado a duplicação de referências e requisitos entre a Lei n.º 32/2008 c o Código de Processo Penal.»

[18] DÁ MESQUITA, 2010; CONDE CORREIA, 2014

[19] CONDE CORREIA, 2014

3. Lei n.º 109/2009 – Lei do Cibercrime

Deixemos para o próximo capítulo a aprofundada análise deste diploma, focando-nos antes, por agora, no lugar que ocupa nesta teia legislativa que compõe o regime probatório digital, a nível de recolha de prova.

Esta lei veio transpor, por um lado, a Decisão Quadro 2005/222/JAI do Conselho, de 24/02/2005, e por outro, adaptar à ordem interna a Convenção.

Neste quadro legislativo importa salientar que esta lei consagra um verdadeiro

> «regime processual penal geral de obtenção de prova digital, potencialmente dirigido a todos os crimes. Desse modo, impunha-se a integração das suas normas no CPP, concretamente no Título III («Meios de obtenção de prova») respetivo Livro II («Da prova») (21). Pelo que só uma intenção mal dissimulada do legislador em ampliar e facilitar os meios de obtenção daquela prova o pode ter levado a optar por produzir (mais) um diploma especial.»[20]

Também João Conde Correia (2014) é crítico deste diploma, que «apesar da sua denominação equívoca e aparentemente restritiva (Lei do Cibercrime), veio acrescentar mais um apertado e desnecessário nó górdio. (…) O legislador nacional consagrou, finalmente, um verdadeiro sistema processual de prova digital.»

Também esta lei veio densificar a legislação extravagante sobre o cibercrime. Tivesse o legislador «optado pelo enquadramento sistemático destas disposições no próprio Código de Processo Penal, talvez se tivessem evitado dificuldades de harmonização com normas do próprio Código (v.g., artigos 179.º e 189.º) e de outros diplomas extravagantes (v.g., normas da Lei n.º 32/2008, de 17 de julho» [21]

Nesta lei, em geral, foram introduzidas na ordem jurídica portuguesa figuras processuais novas e é este é o diploma do qual nos iremos ocupar daqui em diante, que merece análise profunda, a qual não nos propomos a fazer, envergando apenas, e humildemente, pelo exercício de análise crítica do regime de buscas e apreensões como método de obtenção

[20] LOPES MILITÃO, 2012

[21] FIDALGO, 2019

de prova digital em processo penal, procurando salientar os aspetos mais problemáticos, esperando poder fazer parte do caminho para um sistema justo e eficaz.

4. Conjugação

Por fim, cumpre lançar alguma luz sobre esta intrincada amálgama legislativa, com largas zonas «cinzentas de confronto e atrito»[22].

Em primeiro lugar, contrapondo as leis 32/2008 e 109/2009 ao regime constante do artigo 189º do CPP, acompanhamos a tese maioritária que defende que estes diplomas revogam tacitamente as parcelas incompatíveis do regime do CPP.[23] João Conde Correia (2009) explica que «as leis extravagantes se sobrepõem àquele regime geral, que só subsiste naquilo que não foi depois especialmente regulado.» O mesmo autor tece ainda uma dura crítica no mesmo sentido: «Não se compreende (…) porque é que o legislador não o revogou formalmente (…) a sua manutenção formal só pode ser perniciosa.»

Em segundo lugar, e menos consensual, será a conjugação entre as duas leis. A tese maioritária defende uma relação de complementaridade entre ambas, apoiando-se na letra da lei (artigo 11º, nº2 da Lei do Cibercrime.[24] Não temos a certeza se esta será a melhor solução, valendo a pena expor paralelamente o entendimento de João Conde Correia (2009) quando afirma que tal interpretação impõe um ónus demasiado pesado, de determinar os respetivos campos de aplicação de cada diploma, destrincando «campos que parecem sobrepostos, mas são afinal contíguos».

Acompanhamos o mesmo autor, na defesa de uma tese que se afigurará, possivelmente, mais sensata – a de que a Lei do Cibercrime revogou parcialmente a lei 32/2008, na parte em que estabelece o regime de acesso aos dados informáticos, mantendo-se em vigor o que releva ao estabelecimento de deveres dos fornecedores de serviços e prestação de dados – sobrevivendo apenas aquilo «que não foi expressamente regulado pela Lei do Cibercrime» tendo em conta que, de facto, «não há nenhuma razão para manter regimes

---

[22] CONDE CORREIA, 2009

[2323] Neste sentido João Conde Correia (2009), Paulo Dá Mesquita (2010), Rita Castanheira Neves (2011). Em sentido contrário Paulo Pinto de Albuquerque (2011 e 2014), e Pedro Verdelho (2009)

[24] Neste sentido Rita Castanheira Neves (2011), Renato Lopes Militão (2012), e Benjamim Silva Rodrigues (2009)

diversificados de acesso e que, contraditoriamente, oneram a investigação dos crimes mais graves com exigências injustificadas.»[25].

III. A Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro)

1. Breve análise do diploma

Esta lei foi publicada a 15 de setembro de 2009, e pretendeu adaptar, como de resto já vimos, a Convenção ao direito interno. Veio também, tal como consta da Exposição de Motivos da proposta de Lei nº 289/X[26], e que acabou por não ser reproduzida na própria LC, revogar a Lei nº 109/91 (Lei da Criminalidade Informática) que hoje se encontrava obsoleta "pelo decurso de quase duas décadas".

A LC,

para além de visar cumprir as obrigações internacionais do Estado Português, visou também suprir «uma lacuna do direito processual geral em termos amplos e abrangentes da generalidade dos crimes.»

Desta lei anterior muitas incriminações mantiveram-se, ainda que seja patente que com a LC houve uma preocupação em criminalizar a 'produção ou difusão de vírus e outros programas maliciosos'[27]. Porém, não podemos olhar para a LC apenas como uma nova lei de criminalidade informática, uma vez que a LC é uma lei altamente compreensiva a nível de matérias, instituindo um verdadeiro regime processual informático.

O legislador procurou reunir num único diploma todas as normas respeitantes à criminalidade informática: normas de direito substantivo, normas de direito processual e normas relativas à cooperação judiciária em matéria penal. O que significa que a lei do Cibercrime contem disposições introdutórias e definições legais, bem como um capítulo

---

[25] CONDE CORREIA, 2009

[26] Disponível em: https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c637939595447566e4c305276593356745a57353062334e4a626d6c6a6157463061585a684c7a45324f544a684e7a63344c57457a4f4751744e474934595330344d5459304c544d345a4459315a6a59784e444d304f53356b62324d3d&fich=1692a778-a38d-4b8a-8164-38d65f614349.doc&Inline=true

[27] CASTANHEIRA NEVES, 2011

dedicado a normas penais de natureza material, onde são consagrados diversos tipos penais especificamente relacionados com a criminalidade informática; além disso, em capítulo autónomo, e como já se mencionou, um conjunto de normas de natureza adjetiva (designadas como "disposições processuais") consagrando uma série de novos meios de obtenção de prova. Finalmente, um capítulo sobre cooperação internacional, que contém normas que complementam as disposições da Lei da Cooperação Judiciaria em Matéria Penal..

O terceiro capítulo começa, no artigo 11º, com o âmbito de aplicação das disposições processuais, no fundo determinando qual a natureza destas normas. Ocupar-nos-emos da análise deste artigo em subcapítulo autónomo, uma vez que merece uma análise atenta.

Os artigos 12º e 13º elencam regras inovadoras sobre preservação expedita de dados e revelação expedita de dados de tráfego. O artigo 14º segue, adaptando à nossa realidade, o já mencionado instituto da injunção para apresentação ou concessão de dados.

> «O artigo 14.° da lei do cibercrime constitui, tal como as medidas cautelares que o precedem, um dos eixos de revogação do artigo 9.° da Lei n.º 32/2008, de 17-07, pois, além do próprio conceito amplo de «dados informáticos específicos e determinados armazenados num determinado sistema informático», fez menção específica a que a injunção, da competência da autoridade judiciária que dirige o processo, se pode destinar a «dados relativos as suas clientes ou assinantes»[28].

O artigo 15º consagra as pesquisas informáticas. Este artigo dispõe que a autoridade judiciária não só é a entidade competente para autorizar ou ordenar a realização da diligência, como a quela que, sempre que possível, deve presidir às mesmas. Em certos casos os órgãos de polícia criminal podem proceder sem autorização da autoridade judiciária, devendo, porém, a diligência ser-lhe de imediato comunicada. Este artigo, bem como os seguintes, são verdadeiramente o objeto deste estudo, pelo que remetemos para capítulo próprio a sua análise aprofundada.

O artigo 16º dispõe sobre a apreensão de dados informáticos, e o artigo 17º sobre a apreensão de mensagens de correio eletrónico ou registos de natureza semelhante que se

[28] DÁ MESQUITA, 2010

encontrem armazenados em sistema informático alvo de pesquisa informática ou outro acesso legítimo.

O artigo 18º incide sobre a interceção de comunicações, e o artigo 19º sobre ações encobertas.

Por fim existe um capítulo sobre cooperação internacional, seguido do último capítulo referente às disposições transitórias.

Concluímos esta breve introdução à Lei do Cibercrime com uma reflexão de Renato Lopes Militão (2012), que bem introduz uma das fragilidades mais marcantes desta Lei:

> «Evidenciando uma das mais vincadas imagens de marca do processo penal neoliberal, a Lei n.º 109/2009, quer no âmbito das suas normas processuais, quer no da recente cooperação internacional, veio conceder enormes poderes aos órgãos de polícia criminal, relativamente à preservação, pesquisa e apreensão de dados informáticos.»

De resto, cabe aprofundar dois temas um pouco mais a fundo. Por um lado, a opção tomada pelo legislador de consagrar um regime tão importante em diploma extravagante; e por outro, a natureza das normas processuais da Lei do Cibercrime.

2. A opção do legislador de consagração do regime em diploma extravagante – breves considerações.

Obviamente que são já nossos conhecidos todas as vantagens e importância da codificação, o que torna ainda mais complicado compreender a escolha do legislador em «acentuar o atual paradigma de decodificação e de negar a desejável centralidade normativa do CPP, contribuindo assim para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático.»[29].

Como já referimos, não é pacífica a decisão do legislador de consagrar normas de direito probatório de espetro geral num diploma extravagante, em vez de rever e adaptar o CPP

[29] CONDE CORREIA, 2014

aos dias de hoje. Parece, no entanto, que essa decisão foi tomada conscientemente e a justificação exposta na Exposição de Motivos *supra* mencionada. Cumpriria analisar os argumentos a favor desta descentralização normativa, e apreciar o seu mérito, se a envergadura deste estudo o permitisse.

Deixamos apenas nota de que o esforço legislativo dedicado a evitar a consagração deste regime no Código de Processo Penal, parece ter um custo bastante mais elevado do que se simplesmente se tivesse procedido à sua revisão. As dificuldades de conjugação entre este diploma, o CPP, e a lei 32/2008 permanecem, e o peso nos tribunais para proceder a este tipo de exercício que poderia não ser necessário todos os dias aumenta. O legislador permanece indiferente a esta situação, volvidos 13 anos, parecendo continuar a optar por esta contínua descodificação. Tal é particularmente visível se referirmos, um dos elementos mais relevantes deste estudo: a proposta de alteração ao artigo 17º da Lei do Cibercrime.

O legislador, em 2021, com já 12 anos de críticas sobre a dispersão normativa relativa ao regime probatório digital, propôs que se alterasse a Lei do Cibercrime, tentando densificar ainda mais o regime, através de um conjunto de alterações significativas e com implicações constitucionais graves, estabelecendo-o como um dos regimes de maior importância no nosso ordenamento processual penal, com uma das maiores suscetibilidades de violações de direitos fundamentais dos seus visados, mas lutando pela sua permanência num diploma extravagante.

Não compreendemos uma evolução legislativa neste sentido, nem tão pouco, a insistência do legislador neste modelo.

Concluímos assim, acompanhando, uma vez mais, João Conde Correia (2014):

> «A prova digital (…) continua mergulhada num verdadeiro pântano prático, e sobretudo, normativo, que só poderá ser superado mediante uma intervenção legislativa coerente, global, e cientificamente sustentável. O amadurecimento dos conceitos e das necessidades, propiciado pela riqueza da prática jurídica quotidiana e sedimentado por uma longa reflexão doutrinal, já permite, no entanto, abandonar o experimentalismo e a improvisação inicial e substituí-los por um modelo que conjugue a boa técnica com a melhor substância.»

E, Paulo Dá Mesquita (2010) que oferece uma solução:

«(…) nada obsta a que o intérprete aborde o cap. III da Lei do Cibercrime essencialmente como um envergonhado ou escondido novo cap. V («da prova eletrónica») do título III («meios de obtenção de prova») do liv. III («da prova») do Código de Processo Penal ou múltiplas normas integráveis em diferentes capítulos do referido título III sobre meios de obtenção de prova»

3. Natureza das normas da Lei do Cibercrime - como normas de direito probatório de espetro geral aplicável a qualquer crime

Como referimos, abordamos agora um dos aspetos mais relevantes deste diploma. Apesar de ter surgido como uma lei com normas de natureza excecional, orientadas para a investigação de crimes revestidos de especial ofensividade, do espetro cibercriminal, tal não é o caso.

O artigo 11º da LC determina um campo de aplicabilidade de tal forma extenso, estabelecendo regras processuais aplicáveis de forma geral a «um universo de crimes aberto, independentemente dos elementos típicos»[30],

O n.º 1 do artigo 11. ° (âmbito de aplicação das normas processuais) da lei do cibercrime corresponde à transposição das determinações do n.º 2 do artigo 14.° da Convenção. A al. a) não levanta grandes questões.

A al. b), porém, é uma norma geral que prevê a aplicabilidade das regras processuais, para além dos crimes informáticos, a crimes «cometidos por meio de um sistema informático» independentemente da previsão típica do crime. Prevê-se, portanto, a aplicação a um conjunto tão múltiplo de realidades, quanta a criatividade os criminosos tenham para cometer crimes de diversas maneiras. Da nossa parte, entendemos que esta disposição merecia talvez, uma redação mais cautelosa, sob pena de se apresentar como uma norma vaga e indeterminada.

[30] DÁ MESQUITA, 2010

É a al. c) que é a pedra de toque deste preceito, que impõe um verdadeiro regime geral[31] aplicável a qualquer crime, sempre que "seja necessário proceder à recolha de prova em suporte eletrónico".

O Tribunal Constitucional, no enquadramento geral do Acórdão 687/2021[32], procede a uma exímia explicação das implicações desta alínea:

> «(…) tendo em consideração os processos de digitalização e desmaterialização que dominam a sociedade contemporânea, o âmbito de aplicação efetivo das normas adjetivas da Lei n.º 109/2009 revela-se substancialmente mais amplo do que poderia parecer numa primeira análise (…). De facto, a prova em suporte eletrónico tenderá a ser uma realidade material omnipresente na vida comunitária, mais ainda do que já sucedia aquando da aprovação da versão inicial das normas questionadas; notem-se, entre muitos outros fatores de incremento da vida digital, o aumento das interações entre Estado e cidadãos com recurso à Internet, bem como o crescimento do teletrabalho, em particular no cenário pandémico – e estes exemplos constituem apenas duas das mais recentes manifestações da extensão a novos domínios da vida em sociedade das referidas digitalização e desmaterialização. Na presente análise, dever-se-á, pois, ter em atenção que os preceitos questionados são passíveis de aplicação à investigação de qualquer crime, e não apenas aos crimes diretamente relacionados com a utilização da informática.»

Colmatando com uma afirmação que não deixa margem para dúvidas: «Efetivamente, o legislador nacional escolheu, ao aprovar a Lei do Cibercrime, consagrar normas de direito probatório de espetro geral num diploma extravagante, ao invés de rever e adaptar o CPP aos novos tempos.»

É de facto uma verdade incontornável que o impacto que a internet e os sistemas informáticos têm atualmente no dia-a-dia de cerca de quase 9 milhões de portugueses (número que continua a subir a passos largos). Basta pensar que para fazer uso deste

---

[31] Neste sentido Paulo Dá Mesquita (2010), Rita Castanheira Neves (2011), Renato Lopes Militão (2012) e Sónia Fidalgo (2019)

[32] Doravante "O Acórdão"

regime basta que se considerem existir provas digitais que ajudem na busca da verdade material, que tenham de ser recolhidas em suporte digital. Basta pensar que qualquer crime discutido num fórum, planeado num documento, fotografado e guardado num telemóvel – enfim, uma infinita quantidade de situações – para perceber o verdadeiro impacto desta alínea, que em causa está «a criação de meios de obtenção de prova digital para o combate à criminalidade, seja qual for a sua forma (…).»[33].

Acompanhamos Paulo Dá Mesquita (2010) que afirma que

«As regras de direito probatório previstas no diploma não são assim meras normas processuais sore cibercrimes ou sequer apenas relativas a crimes praticados em sistemas informáticos, mas correspondem a um regime consideravelmente mais abrangente sobre prova eletrónica em processo penal aplicável a qualquer crime.»

Ou seja, «todas aquelas medidas e obrigações podem ocorrer irrestritamente na investigação da generalidade dos tipos criminais, independentemente da moldura penal ou da natureza destes. Processos de pequena criminalidade ou referentes a crimes semipúblicos e, mesmo, particulares admitem, pois, essas medidas.»[34].

Em causa está, então, um verdadeiro regime geral dirigido à obtenção de prova digital em processo penal, aplicável à generalidade dos crimes. Tal conclusão enfatiza a importância deste estudo – os métodos de obtenção de prova sob análise podem ser usados transversalmente, em relação a todos os crimes previstos no Código Penal. A importância da sua cuidada e exímia legislação é tão grande quanto o seu campo de aplicação.

[33] VENÂNCIO, 2011

[34] LOPES MILITÃO, 2014

IV. Objeto de estudo – buscas informáticas e subsequentes apreensões de dados informáticos - regime atual

A. A busca informática: artigo 15º - novo nome para antiga diligência

É o artigo 15º da Lei do Cibercrime o objeto primário deste estudo. Este preceito estabelece o regime jurídico das buscas informáticas. É um artigo inovador quanto ao conteúdo, mas não quanto ao tipo de diligência que representa.[35]

Denominado "pesquisa de dados informáticos" este artigo estabelece verdadeiramente o regime das buscas em sistema informático[36]. Esta nova expressão foi adotada pela lei "para aquilo que poderia designar-se busca informática."[37] [38]

Como explica Pedro Verdelho (2009),

> "(…) estas aparentemente novas medidas processuais coincidem, no ambiente do ciberespaço, com os clássicos meios de obtenção de prova. Assim, a pesquisa de dados informáticos corresponde claramente à busca e a forma como está descrita inspira-se clara e assumidamente no artigo 19º da Convenção sobre o Cibercrime (que, aliás, lhe chama precisamente «buscas ou de outro modo aceder a um sistema informático»)"

Na mesma linha, Rita Castanheira Neves (2011) refere que "(…) a pesquisa de dados informáticos consagrada no artigo 15. ° da Lei do Cibercrime consiste nas tradicionais buscas previstas nos artigos 174.° e segs. do Código de Processo Penal, mas adaptada à criminalidade informática ou a casos em que se mostra indispensável recorrer à prova digital."

Refere Duarte Nunes Rodrigues (2018) que:

> "A previsão, na CCiber, da pesquisa de dados informáticos visou modernizar e harmonizar as legislações nacionais em matéria de busca e apreensão, para fins de investigação criminal, de dados informáticos armazenados, pois, em

[35] Neste sentido, Pedro Verdelho (2009)

[36] Razão pela qual optamos, neste estudo, por acolher a expressão "busca informática", havendo no entanto quem opte pela denominação "buscas digitais".

[37] FIDALGO, 2019

[38] No mesmo sentido, também, Ana Luísa Pinto (2005 e 2007), João Conde Correia (2014); entre outros.

> muitos países, os dados informáticos (que são realidades intangíveis) apenas poderiam ser obtidos da mesma forma que os bens corpóreos (i.e. através da obtenção do suporte no qual se encontram armazenados os dados e, como tal, mostrava-se necessário prever a busca e apreensão de realidades intangíveis, como são os dados informáticos. (…) Na pesquisa de dados informáticos (cujos cânones foram pensados para a obtenção de realidades intangíveis), ainda que se mantenham muitas das características das buscas "tradicionais", mostra-se necessária a previsão de regras complementares para assegurar que os dados informatizados podem ser obtidos com a mesma eficácia de uma operação de busca e apreensão de suportes de dados tangíveis."

Este preceito estabelece que quando, "no decurso de um processo, se torne necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência."

Consiste no fundo, o regime, em permitir às autoridades competentes o acesso a um sistema informático, "a fim de nele localizarem (e, posteriormente, procederem à respetiva apreensão) dados informáticos nele armazenados", sendo que esta pesquisa pode incidir sobre "a totalidade do sistema informático, uma parte do sistema informático (v. g. um dispositivo de armazenamento de dados a ele conectado) ou um suporte de armazenamento de dados independente (u. g. uma pen drive)."[39].

De facto, e nas palavras de Paulo Dá Mesquita (2010), apesar da peculiaridade terminológica, são igualmente validos os parâmetros constantes do artigo 174º nº1 do CPP relativamente às buscas em sentido tradicional: i) quando existirem indícios de que dados informáticos relacionados com um crime ou que possam servir de prova se encontram num determinado sistema informático, deve ser ordenada busca informática; e ii) a busca informática é ordenada por despacho pela autoridade judiciária competente, devendo esta sempre que possível, presidir à diligência. Este autor defende ainda que

[39] RODRIGUES NUNES, 2018

apodar este meio de obtenção prova como pesquisa não altera a sua verdadeira natureza processual de busca.

No fundo, não parece razoável a escolha do legislador de uma nomenclatura diferenciada para uma realidade que é una. Evidentemente que quando se trata de uma busca informática, existem especificidades, e estas devem ser acauteladas por um regime específico, pensado em concreto para esta realidade. Neste sentido Pedro Verdelho (2009) quando diz que "todas estas normas têm como tónica comum pretenderem adaptar para o ambiente digital (…) as clássicas diligências de busca (…)" e "(…) esta adaptação (…) dos regimes criados [é imposição] da especificidade da criminalidade a cuja investigação se dirigem."

No entanto, parece-nos que é crucial manter o verdadeiro nome do meio de obtenção de prova, sob pena de se acabar por distanciar dos princípios essenciais que regem a busca, quer seja ela tradicional ou informática.

Veremos, de seguida, quais as especificidades em causa e que dificuldades representam face ao regime tradicional. Bem como se imporá, certamente, uma comparação destes dois regimes, e a ponderação de qual o regime tradicional de buscas que mais se assemelha ao das buscas informáticas, procurando perceber se o regime efetivamente mais próximo partilha com este novo regime as salvaguardas mais relevantes em matéria de proteção dos direitos dos arguidos, e pessoas alvo das buscas, ou se por outro lado, este afastamento de nomenclatura é acoplado de um afastamento dos direitos associados.

1. Dificuldades acrescidas face ao regime tradicional

O primeiro ponto a referir, a nível de requisitos das buscas informáticas, decorre do nº6 do artigo 15º da LC. Trata-se de uma remissão para o CPP, das regras de execução de buscas, com as necessárias adaptações. Assim, não é difícil desenhar um quadro de requisitos bastante próximo do regime tradicional previsto no CPP.

Estabelece, nomeadamente o artigo 174º, nº2 do CPP, que "quando houver indícios de que os objetos referidos no número anterior (relacionados com um crime ou que possam servir de prova], ou o arguido ou outra pessoa que deva ser detida, se encontrem em lugar reservado ou não livremente acessível ao público, é ordenada busca".

É relevante, porém, explicitar certos aspetos próprios deste regime, bem como as dificuldades específicas do mesmo.

a. Requisitos próprios

i) Determinabilidade

Ainda assim, a muitas destas dificuldades práticas subjazem soluções que se prendem com o rigor jurídico associado aos requisitos para efetuar este tipo de diligências. Vejamos como o critério da determinabilidade, e de seguida, do grau de necessidade, pode ser útil para facilitar todo o processo de obtenção de prova digital através de buscas informáticas.

Nos Estados Unidos da América decorre da 4ª emenda que todos os mandados de busca descrevam com particularidade dois elementos: i) o sítio a ser alvo de busca, e ii) as coisas específicas a ser apreendidas em resultado da busca. Este *"particularity requirement"* é um dos pilares mais importantes na base de qualquer mandado de busca. Na busca informática afigura-se ainda mais relevante.

Em Portugal, também é claro que o critério da determinabilidade existe. Consta diretamente do artigo 15º, nº1 da LC que o objetivo de uma busca é obter "(…) dados informáticos **específicos e determinados**, armazenados num determinado sistema informático (…)"[40]. A mesma lógica aplicar-se-á, portanto, quanto a este requisito, em Portugal como nos EUA.

Michael W. Bailie, Ed Hagen e Marshall H. Jarret (2009) explicam com bastante precisão em que consiste propriamente esta determinabilidade:

> «Descrever com particularidade as "coisas a serem apreendidas" tem dois elementos distintos. Primeiro, o mandado deve descrever as coisas a apreender com linguagem suficientemente precisa para que diga aos oficiais como separar devidamente os itens sujeitos a apreensão dos itens irrelevantes; Segundo, a descrição das coisas a apreender deve ser limitada ao âmbito da causa provável estabelecida no mandado. Considerados em conjunto, os elementos proíbem os agentes de obter "mandados gerais" e, em vez disso, exigem que os agentes efetuem apreensões estritas que tentam minimizar intrusões injustificadas na privacidade. (…) O mandado deve identificar essa

[40] Sublinhado nosso.

> informação com particularidade, concentrando-se no conteúdo dos ficheiros relevantes e não nos dispositivos de armazenamento que os possam conter (...).
>
> Os agentes devem ser particularmente cuidadosos quando procuram autoridade para apreender uma ampla classe de informação (...) não podem simplesmente solicitar autorização para apreender "*todos os registos*" (…) Uma frase igualmente perigosa [é] "*todos e quaisquer dados, incluindo, mas não limitados a (...)*" que já foi considerada pelos tribunais como sendo uma frase usada para transformar um mandado de busca informática num mandado geral inconstitucional (…)»[41]

Ainda dentro do quadro doutrinal norte americano John J. Farmer Jr. (2000) refere que à medida que a quantidade de informação que é possível armazenar num computador aumenta exponencialmente (afirmação feita em 2000, que hoje se revela não só acertada, como ainda relevante) se torna difícil a busca e apreensão de informação com relevância probatória, e que é neste âmbito que o critério da determinabilidade (ou da particularidade, numa tradução direta deste autor) é mais importante. Este autor relembra a dificuldade acrescida de precisar o local alvo de buscas quando se trate de uma busca informática, tendo em conta que a informação guardada num computador pode estar ligado a outros computadores e servidores num local específico ou fora do mesmo local. É o critério da determinabilidade que vai auxiliar no sucesso de execução de um mandado de busca informática, por criar a necessidade de a autoridade que o requisita saber exatamente o que quer procurar, e onde deve procurar.

Vânia Costa Ramos (2006), invocando a jurisprudência dos tribunais superiores alemães, também, reflete sobre esta questão. Diz a autora que "Deve (…) evitar-se a obtenção excessiva de dados sem qualquer importância para o processo – a apreensão da totalidade dos dados constantes de um computador, ou do aparelho em si, para obtenção dos dados de ligação, será em regra, desnecessária, bastando o exame destes *in loco*."

ii) Competência

A nível de competência apenas uns apontamentos se impõem. Em primeiro lugar, a regra geral é de que, a competência para autorizar o recurso à pesquisa de dados informáticos é da autoridade judiciária (nos termos do artigo 15.°, n.º 1, da Lei do Cibercrime), sendo portanto[42], a competência para emitir tal ordem do magistrado do Ministério Público na fase do inquérito, do Juiz de Instrução Criminal na fase da instrução e do Juiz na fase de julgamento.

Por aplicação subsidiária do regime tradicional podemos também acompanhar Duarte Nunes Rodrigues (2018) em como nos casos em que a busca incida sobre sistemas informáticos utilizados para o exercício de uma atividade sujeita a sigilo profissional, a competência é do Juiz (que deverá igualmente presidir à diligência), nos termos dos artigos . 268.°, n.º 1, al. c), e 177. °, n.ºs 5 e 6, do CPP, e que em situações em que se proceda a uma pesquisa "presencial" num sistema informático que se encontra num local abrangido pela tutela jurisdicional do direito à inviolabilidade do domicilio, a entrada nesse espaço depende, obviamente, e nos moldes típicos, de autorização judicial.

Uma nota importante sobre a competência prende-se com o n.°3 do art.15º da LC. O legislador determina que a pesquisa poderá ser realizada pelo Órgão de Polícia Criminal sem prévia autorização da autoridade judiciária[43] em duas situações:

(1) mediante o consentimento[44] de quem tiver a disponibilidade ou controlo dos dados informáticos em causa (devendo o consentimento ficar, por qualquer forma, documentado) ou

(2) em casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

Formulamos algumas considerações quanto a este nº3.

Quanto à primeira situação, Benjamim Silva Rodrigues (2009) tece duras críticas à exceção aberta pelo legislador. Entende o autor que esta alargamento da competência a

---

[42] Conjugando essa norma com o art. 1.°, al. b), do CPP.

[43] Sublinhado nosso.

[44] Sublinhado nosso.

estes órgãos não é compatível com o "paradigma constitucional e legal de restrição de direitos fundamentais" indo tão longe quanto dizer que podendo recair suspeitas já formuladas sobre a pessoa que tem o controlo dos dados em causa, os Órgãos de Polícia Criminal poderão "de forma desleal, sobrestar na sua constituição como arguido para, desse modo, sem a informar do direito de prestar ou não essa colaboração, obter informações autoincriminatórias que jamais poderiam obter de outra forma".

Não acolhemos necessariamente esta visão, ainda que também não descuremos que possa representar uma percentagem das situações práticas e que de facto, a questão do consentimento levanta vários problemas, que abordaremos de seguida. Acompanhamos, então, Duarte Rodrigues Nunes (2018), em sentido contrário quando refere que

> "num estado de direito terá de existir um mínimo de confiabilidade nos [órgãos de polícia criminal] e, por isso, não vigora entre nós qualquer princípio da desconfiança no labor das autoridades policiais e a presunção da inocência não impõe qualquer "presunção" de ilegalidade da atuação das autoridades judiciárias"

Quanto à segunda alínea Benjamim Silva Rodrigues (2009) apresenta novamente uma crítica que também não podemos acolher, mas que consideramos pertinente chamar à atenção. Entende o autor que estaremos neste caso perante um "direito processual penal do inimigo" e perante o "desapossamento dos níveis democráticos mínimos de garantia dos seus direitos fundamentais à luz das legítimas expectativas e garantias processuais penais (…)".

Mais uma vez, acompanhamos Duarte Rodrigues Nunes (2018), em sentido contrário, ao referir que o *ratio* da norma é a existência de um certo *periculum in mora* quer relativa à eficácia da investigação, quer a potenciais vítimas cuja proteção é essencial.

No fundo, o entendimento que fazemos do pensamento de Benjamim Silva Rodrigues é somente o de que não repugna a ideia de que a busca informática não deveria poder ser uma competência dos Órgãos de Polícia Criminal, sem prévia autorização da autoridade competente. Pese embora os argumentos sustentados pelo autor sejam demasiado austeros, a verdade é que se abrem as portas a um conjunto de situações demasiado amplas, e se esse é um risco que aceitamos que se corra em salvaguarda dos interesses que a alínea b) visa proteger, já não estaremos tão certos quanto à alínea a).

2. Artigo 15º, nº5

O nº5 do artigo que estabelece o regime da busca informática representa uma novidade e uma verdadeira especificidade deste regime, face aos tradicionais – ainda que pela natureza desmaterializada e descentralizada do objeto da busca – e merece um apontamento, uma vez que em causa está um mecanismo que não é pacífico na doutrina.

O nº5 transpõe o nº2 do artigo 19º da CCiber, ou pelo menos transpõe o mecanismo previsto na CCiber – trata-se da possibilidade de estender a busca informática efetuada num sistema informático, a outros sistemas ou a uma parte diferente do mesmo sistema, se houver razão para crer que os dados procurados lá se encontram, partindo do pressuposto que a busca inicial é legítima, e mediante autorização ou ordem da autoridade competente.

Acontece, porém, que o artigo 19º da CCiber contém uma menção específica ao território nacional[45], limitando, assim, este mecanismo no espaço. Ao transpor o mecanismo para a ordem jurídica interna, o legislador português optou por eliminar a referência ao "seu território" criando dúvidas acerca da aplicação do mecanismo. O entendimento acolhido terá, naturalmente, implicações a nível de cooperação internacional entre estados. Não pretendemos, neste âmbito, proceder a uma análise do tema, tão só identificá-lo, deixando para momento posterior a sua cuidada reflexão.

B. Apreensões de dados informáticos, correio eletrónico e registos de comunicações de natureza semelhante – os artigos 16º e 17º

Uma vez mais, o regime agora sob apreço não nos é estranho. A apreensão é um método de obtenção de prova constante do CPP há vários anos, pelo que esta "nova" realidade

[45] "(…) sempre que as suas autoridades efectuem buscas ou de outro modo acedam a um determinado sistema informático ou a parte dele, em conformidade com o disposto na alínea a) do n.º 1 do presente artigo, e caso existam motivos para crer que os dados procurados estão armazenados noutro sistema informático ou em parte dele**, situado no seu território**, e que é possível aceder legalmente a esses dados ou que eles estão disponíveis através do primeiro sistema, as autoridades são capazes de rapidamente alargar a busca ou o acesso equivalente ao outro sistema (…)" (sublinhado nosso)

representa somente um desvio ao regime geral, que não se afasta, contudo, dos seus pressupostos base e traços gerais.

A lei do cibercrime estabelece o regime das apreensões direcionado ao ciberespaço, às apreensões de dados informáticos (artigo 16º) e ainda, afastando-se do preceituado na CCiber , prevê uma circunstância específica relativa à apreensão de um conjunto de dados informáticos sob a forma de "comunicação e registos de natureza semelhante".

1. Artigo 16º - apreensões de dados informáticos

O nº1 do artigo 16º estabelece os pressupostos base em que pode ocorrer uma apreensão de dados informáticos, referindo especificamente a necessidade probatória, com vista à descoberta da verdade, e como já afirmámos, «apesar de algumas inovações em termos de verbalização das regras (artigo 16.°), não se alteram os pressupostos funcionais da apreensão em processo penal (cf. artigo 178., nºs 1 e 3, do CPP)» (DÁ MESQUITA, 2010). Assim, podem ser apreendidos dados informáticos que i) tenham servido ou estivessem destinados a servir de base à prática de um crime; ii) tenham sido deixados pelo agente no local do crime; iii) quaisquer outros suscetíveis de servir a prova. A nível de competência também não acarreta grandes novidades face ao regime tradicional, competindo a autorização, ordem ou validação por despacho, à autoridade competente que será o Ministério Público na fase de inquérito, o JIC na fase de instrução e o Juiz na fase de julgamento.

O nº2 estabelece a possibilidade de delegação dessa competência nos OPCs, sem previa autorização judicial se ocorrer no âmbito de uma busca legitimamente ordenada e executada, bem como na circunstância de haver perigo ou urgência na demora – mais uma vez aceitamos o critério do *periculum in mora* para legitimar esta atuação dos OPCs. Temos dúvidas acerca da apreensão por parte de OPCs que resulte de busca executada nos termos excecionais do artigo 15º, nº4, a), por maioria de razão decorrente das teorizações já prestadas no capítulo anterior.

No nº3, o legislador estabelece uma salvaguarda de proteção dos dados mais pessoais dos visados: "caso 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, sob pena de nulidade esses dados ou documentos são

apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto" (artigo 16.º, n.º 3).

Assim,

> «Sempre que na fase de inquérito foram apreendidos, por exemplo, filmes, fotografias ou gravações sonoras que possam pôr em causa a privacidade dos sujeitos, o juiz de instrução deverá proceder a uma ponderação de interesses no caso concreto: por um lado, o interesse na salvaguarda da privacidade, por outro lado, os interesses que a investigação criminal visa prosseguir.»[46].

A nível de modos de apreensão, o legislador estabeleceu quatro: i) apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura; ii) realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; iii) preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou iv) eliminação não reversível ou bloqueio do acesso aos dados. Sónia Fidalgo (2019) esclarece que na verdade, apenas os dois primeiros procedimentos são verdadeiras apreensões, sendo que os últimos dois consubstanciam meios de proteção da prova ou da disposição original dos dados no sistema. De facto, não se compreende a razão pela qual o legislador optou por estabelecer no mesmo preceito procedimentos diferentes, com objetivos diferentes, e que deveriam acarretar cautelas diferenciadas.

Acompanhamos, então, a crítica tecida por Paulo Dá Mesquita (2010) em como este conjunto de formas de apreensão revela as «(poucas) preocupações de rigor conceptual da lei (…)» uma vez que agrega um conjunto de «(…) realidades materiais, semântica e juridicamente inconfundíveis.» num único regime de apreensão de dados informáticos.

Após a apreensão, pelo menos nas primeiras duas vertentes desta figura, existem ainda cautelas a ter, que a nosso ver deveriam constar, também, da lei, uma vez que este momento posterior – o exame forense aos dados apreendidos - é tão ou mais importante como o momento da própria apreensão. É nestes momentos subsequentes que se vai cristalizar a idoneidade da prova obtida, ou não. Um erro neste âmbito pode inutilizar meses de investigação, e o momento da busca e apreensão. «Este passo é de extrema

[46] FIDALGO, 2019

importância para conseguir carrear prova que, direta ou indiretamente, implique ou ilibe o buscado da prática de um crime.»[47].

Na prática este procedimento

> «(…) consiste na realização de uma imagem do suporte fisico apreendido (…) é a partir desta imagem (ou clone - sendo esta a expressão mais apropriada) que se vai desenrolar todo o procedimento pericial conducente à elaboração do relatório de exame pericial. Com a vantagem de esta imagem ser realizada com bloqueador de escrita, ou seja, de se preservar toda a informação que existia no suporte original à data da sua apreensão, não havendo qualquer alteração/adulteração de dados.»

Em suma, o artigo 16º não apresenta grandes dificuldades interpretativas, ainda que não tenha a redação mais feliz, pecando por excesso ao englobar realidades multiplas num só regime. É no artigo 17º que o regime das apreensões se complica, desnecessariamente, como veremos de seguida.

2. Artigo 17º – apreensão de correio eletrónico e registos de comunicações de natureza semelhante

O artigo 17º, ainda incidindo sobre a matéria das apreensões, estabelece um regime especial que se afasta do disposto na CCiber como já vimos. O legislador português optou pela criação desta norma, cuja interpretação tem "(…) gerado dificuldades de compatibilização com o disposto no Código de Processo Penal e tem dado lugar a interpretações doutrinais e jurisprudenciais diversas, sobretudo quando a apreensão se faz na fase de inquérito." [48].

Dispõe o artigo que no âmbito de uma busca quando se encontrem "(…) mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande

[47] DIAS RAMOS, 2017

[48] FIDALGO, 2019

interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.".

Quanto a este regime especial várias questões se levantam, em especial e de maior dimensão, é a discussão relativa à remissão para o regime tradicional da apreensão de correspondência e querela adjacente sobre o correio eletrónico aberto ou fechado, ou em outras palavras, lido ou não lido. Quanto a este segundo tema remetemos para momento posterior. Quanto ao primeiro debruçar-nos-emos já, ainda que de forma sucinta pelas limitações desta exposição.

A questão central no que concerne à razoabilidade desta remissão prende-se com o entendimento que sobrescrevermos relativo à correspondência eletrónica, nomeadamente se consideramos que esta última carece de mais, menos ou a mesma tutela que a primeira.

Um primeiro ponto, automaticamente, é o da redução do âmbito objetivo e subjetivo destas apreensões. No regime tradicional constante do CPP,

> "(…) a apreensão de correspondência só é meio de obtenção de prova admissível para crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos; na LCC, não há catálogo por força do expressamente previsto no artigo 11.º, aplica-se a processos relativos a crimes (a) previstos nessa lei, (b) cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, ou seja, em abstrato, a todos os tipos de crime; No CPP, a correspondência tem de ser expedida pelo suspeito/arguido ou lhe ser dirigida, mesmo que sob nome diverso ou através de pessoa diversa; na LCC, pode respeitar a qualquer pessoa (mais uma vez, o artigo 11.º não faz qualquer restrição de âmbito subjetivo)." [49].

Aproveitamos, uma vez mais, para relembrar que, de facto, o âmbito de aplicação da LC e dos métodos de obtenção de prova nela contidos, não tem qualquer catalogação, abrindo estas possibilidades a um conjunto sem fim de realidades, podendo ser usada em qualquer processo, por qualquer crime, em relação ao qual seja necessário proceder à recolha de prova em suporte eletrónico, em qualquer processo penal, independentemente da

[49] CARDOSO, 2021

gravidade do crime investigado. Foi, portanto, uma evidente opção "(…) do legislador permitir a apreensão de correio eletrónico e registos de comunicações de natureza semelhante sem a limitação[50] decorrente de o crime ser punível com pena de prisão superior a 3 anos."

A remissão para o regime da apreensão da correspondência tradicional é, portanto, da maior importância, uma vez que em causa está um conjunto de situações ilimitado.

O ponto de partida desta questão é que ao correio eletrónico se poderiam aplicar três regimes diferentes: o regime da apreensão de correspondência tradicional (como é atualmente), o regime geral da apreensão de dados informáticos, ou um terceiro regime que ainda não existe mas que poderia ser criado "à medida" para o correio eletrónico, que carece de várias espcificidades, sem dúvida alguma.

Porém, este regime ideal, criado para esta realidade espcífica tendo em conta todas as contigências associadas, não existe. Pelo que a escolha terá de ser entre estes primeiros dois regimes, que de facto existem, e têm características bastante diferentes. Antes de mais, a questão óbvia é que o regime da apreensão de correspondência é bastante mais garantístico, e tutela adequadamente os direitos em causa, algo que já estabelecemos que o regime geral das apreensões carece.

O regime das apreensões de correspondência justifica-se uma vez que é necessária a tutela acrescida deste tipo de dados (comunicacionais) que advém de comunicações ou são em si mesmos comunicações. Este regime representa uma importante limitação à ingerência nas telecomunicações. "A inserção na categoria das telecomunicações é (…) determinante da aplicação ou não do regime específico da interceção de telecomunicações. Aplicando-se este regime, o investigador criminal deparar-se-á com uma limitação na obtenção daqueles dados (…)"[51].

Precisamente por ser uma comunicação eletrónica o tratamento deverá ser mais garantístico, e não o inverso, uma vez que as comunicações em causa são por natureza

[50] Sublinhado nosso.

[51] COSTA RAMOS, 2006

mais vulneráveis. As necessidades de tutela são mais exigentes. Vejamos, um email guardado pode revelar o remetente, o destinatário, o contacto de ambos, a localização de ambos através do endereço de IP, a conversa anterior que se encontrará associada – enfim, um conjunto de informação sobre duas ou mais pessoas que uma carta escrita em papel nunca poderá revelar. Desde já uma carta em papel pode sempre ser anónima, algo que um email nunca poderá ser. A nível de intromissão estadual, também o correio eletrónico se afigura mais vulnerável. Uma carta fisica, assim que lida pelo seu destinatário poderá ser destruída – queimada, rasgada, desfeita – algo que uma comunicação informática nunca poderá ser. É impossível destruir um email ou uma comunicação semelhante – nada se apaga completamente da internet. Assim, e antecipando um dos argumentos contra a diferenciação entre comunicação eletrónica lida/não lida, uma mensagem eletrónica mesmo que já tenha sido lida e permaneça arquivada no servidor de email, ou no próprio computador, mantém a mesma necessidade de proteção contra eventuais ingerências, uma vez que o detentor não tem possibilidade de apagar, e a mensagem contém dados que vão para além dos dados normais constantes de uma carta tradicional.

No fundo, acreditamos que há varíadissimas razões que justificam a tutela acrescida que a remissão para o regime geral da apreensão de correspondência representa, ainda que acreditemos que um regime autónomo fosse preferível.

A doutrina, porém, diverge quanto a esta questão, solidificando ainda mais a querela quanto ao correio aberto ou fechado. Efetivamente, quem defende essa dicotomia entenderá que se deverá aplicar o regime geral da apreensão de dados informáticos ao correio aberto, ou já lido, e inversamente se deverá aplicar o regime da apreensão de correspondência ao correio fechado ou não lido.

A questão do correio eletrónico aberto ou fechado, ou lido ou não lido, reveste a maior importância, uma vez que quem defende que essa dicotomia existe[52] considera que ao correio eletrónioco já lido/aberto se deverá aplicar o regime da simples apreensão, e não o regime do artigo, relativo à apreensão de correspondência.

[52] Neste sentido Rita Castanheira Neves (2011), João Correia Conde, Paulo Dá Mesquita, Tiago Caiado Milheiro, e Duarte Rodrigues Nunes.

Quanto ao correio tradicional, “O Código de Processo Penal não o diz expressamente, mas tanto a doutrina como a jurisprudência, assumem que este regime apenas se aplica para a correspondência fechada. A correspondência aberta tem igual tratamento como se de um documento se tratasse.”

Ora, é evidente que estamos perante realidades distintas e que no que toca ao correio eletrónico, quer falemos de emails, ou de SMS, afigura-se praticamente impossível saber se uma menagem foi lida ou não pelo seu destinatário. Poderemos saber se uma mensagem está “aberta ou fechada”, mas também nada implica que sempre tenha estado nesse estado.

Neste sentido, Armando Dias Ramos: “É difícil saber se uma mensagem foi lida ou não, pois não existem programas informáticos forenses que determinem essa operação, existindo sempre a possibilidade de marcar uma mensagem como "não lida", mesmo após ter sido lida. (…)” O autor remata este pensamento concluindo que “(…) não é o nome dado a um programa informático que faz com que se atribua qualquer equiparação com o correio tradicional.”.

De facto, consideramos que as mensagens podem ser recebidas e reencaminhadas sem se abrirem, sem se ler o conteúdo. Podem ficar armazenadas para ler depois, podem ser lidas e ser sinalizadas como “não lidas” por qualquer razão organizacional da pessoa que recebeu.

Para mais, o correio eletrónico pode ser recebido simultaneamente em várias plataformas, nas quais vai ser considerado lido/não, lido dependendo das circunstâncias concretas, implicando que se possa tutelar juridicamente uma comunicação como não lida, quando na verdade o sujeito já teve conhecimento do seu conteúdo, num outro dispositivo.

Neste sentido Rui Cardoso (2021): “O artigo 17º LCC não faz qualquer distinção (…). As mensagens lidas/não, lidas não são formas de proteção da comunicação. Não são envelopes ou invólucros das mensagens, mas simples filtros que o utilizador pode definir

(de acordo com as suas preferências ou critérios) para mais facilmente gerir o volume de mensagens de correio eletrónico recebidas."[53]

Rita Castanheira Neves (2011) a este propósito considera que "embora a nova lei não tenha sido cabalmente esclarecedora quanto á delimitação da extensão da comunicação eletrónica, dizendo expressamente a partir de que momento é que se considera que a comunicação cessou (…)". É precisamente este entendimento que aceitamos, ainda que em sentido contrário. De facto, a lei não estabelece essa delimitação, nem tão pouco estabelece qualquer distinção entre o correio aberto ou fechado. O legislador incorporou no texto um artigo específico relativamente ao correio eletrónico, que ainda que com alguns problemas interpretativos, não levantou este em particular. Não houve qualquer intenção do legislador em criar esta distinção.

Acompanhamos Sónia Fidalgo quando refere que "O legislador, reconhecendo o anacronismo e a inadequação daquela distinção de regimes, optou por atribuir uma tutela acrescida à mensagem em formato digital, submetendo-a ao regime do artigo 17.º, independentemente de ter ou não sido lida pelo seu destinatário. Tem sido este, também, o entendimento da nossa jurisprudência[54]"[55]

Em suma, não acreditamos que faça sentido essa dicotomia. Não decorre da lei, e serve somente para complicar acrescidamente uma questão que em si mesma, já não é simples.

É também este o entendimento do Tribunal Constitucional[56] que determinou que "(…) desconsidera a distinção entre correio eletrónico lido e não lido pelo destinatário, com suporte na letra do artigo 17.º da Lei do Cibercrime, que não contém qualquer divisão concetual ou de âmbito de aplicação; justifica-se esta orientação, desde logo, com as dificuldades técnicas e a possibilidade de equívocos que tal diferenciação comporta. (…) Por esta razão, e atendendo igualmente aos bens jurídico-constitucionais e aos direitos

[54] Acórdão citado pela autora: Acórdão do Tribunal da Relação de Lisboa de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1)

[55] No mesmo sentido David Silva Ramalho (2014)

[56] Acórdão do Tribunal Constitucional nº 687/2021

fundamentais em causa, bem como à necessidade de uma compreensão atualista da tutela jusconstitucional conferida pela CRP nesta matéria, atender-se-á ao regime jurídico de apreensão de correio eletrónico sem proceder a este tipo de distinções."

Assim, não é dificil aceitar a solução dada pelo legislador com esta remissão do artigo 17º da Lei do Cibercrime para o regime tradicional de apreensão de correio. Em sentido contrário Rita Castanheira Neves (2011) entende que a remissão não tem lógica, uma vez que em causa estão realidades incompatíveis. Não descuramos as implicações práticas sublinhadas por esta autora, mormente no que concerne à dificuldade de que

> "(…) o juiz de instrução que tivesse autorizado ou ordenado a diligência tivesse forçosamente que ser a primeira pessoa a tomar conhecimento de todas as mensagens de e-mail. Para mais, também não é possível imaginar que, depois de se apreciar do não relevo para a prova, o correio electrónico possa ser "restituído" ao visado pela diligência, pois não se pode restituir correspondência virtual que foi gravada para ser levada ao juiz, mas que, no fundo, nunca saiu do computador / espaço virtual onde se encontrava."

Esta dificuldade leva-nos a uma outra dúvida que se prende com a exigência, ou não de um despacho judicial prévio que autorize ou ordene a apreensão de mensagens de correio eletrónico.

Por um lado há quem defenda que é requisito essencial o despacho judicial prévio, nomeadamente por referência à remissão que é feita para o regime tradicional, onde é esse o caso.

Por outro lado, há também quem entenda que a LC não é expressa nste ponto e aceita que se faça a apreensão, sendo posteriormente levada ao juiz que autorizará, ou não a própria apreensão formal. Esta posição é bem explicitada por Rui Cardoso (2021) ao referir que

> "Contrariamente ao que sucede nos casos a que se refere o artigo 16.º, n.º 3, as mensagens de correio electrónico ou semelhantes não estão formalmente apreendidas, pois tal só sucederá se o juiz o determinar. Porém, por regra, tais dados terão já sido objecto de algum dos tipos de apreensão material previstos

> no artigo 16.º, n.º 7, supra analisados, pois só assim haverá "algo" a apresentar ao juiz."

Pedro Verdelho (2009) fala, neste âmbito, numa apreensão cautelar ou provisória sendo que as mensagens só serão efectivamente apreendidas e juntas ao processo se o juiz assim determinar. Se o juiz não autorizar a apreensão, então "a apreensão não se mantém, devendo o suporte das mensagens em causa ser devolvido ou, se a apreensão tiver sido feita por cópia, destruído". No entanto, a verdade é que na prática, para levar ao juiz a comunicação, ou semelhante, encontrada, terão os OPCs ou o MP que ter analisado previamente, e essa informação já servirá para enviesar a investigação, mesmo que o juiz venha a considerar que não deve ser junta aos autos.

Não ignoramos a praticalidade da solução de Pedro Verdelho, e de quem a acompanha, porém não podemos satisfazer-nos com facilidades práticas, que ponham em causa os direitos dos arguidos e visados. Em linha com Sónia Fildago (2019) consideramos que

> "Para além da remissão para o regime da apreensão de correspondência previsto no Código de Processo Penal (artigo 179.º, n.º 1), o próprio artigo 17.º da Lei do Cibercrime estabelece que quando forem encontrados mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova. A lei exige claramente um despacho judicial prévio a qualquer apreensão. **Poderá questionar-se as dificuldades que tal exigência levanta na prática, mas não poderá dizer-se que a lei não faz esta exigência.**[57] Esta tem sido, também, a posição da nossa jurisprudência[58]"

[57] Sublinhado nosso.

[58] Acórdão do Tribunal da Relação de Guimarães de 29-03-2011 (Processo n.º 735/10.0GAPTL-A.G1) e os Acórdãos do Tribunal da Relação de Lisboa de 11-01-2011 (Processo n.º 5412/08.9TDLSB-A.L1-5), de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1) e de 06-02-2018 (Processo n.º 1950/17.0T9LSB-A.L1-5)

Em suma, ainda que admitamos as dificuldades práticas desta remissão para o regime da apreensão de correspondência tradicional esta consta da lei, e deverá, até à formulação de um regime próprio, específico e adequado à realidade do ciberespaço, ser respeitada. Assim, não se concebe que se façam alterações práticas que desprotejam ainda mais o visado.

V. Regime proposto – redação proposta para o artigo 17º[59]

Como já tivemos oportunidade de explicar, em 2021 o Governo veio, no Decreto n.º 167/XIV, propor uma alteração ao artigo 17º da Lei do Cibercrime, que acabámos de analisar, e que visava o seu esclarecimento.

Esta tentativa (frustrada) de alteração legislativa é relevante, uma vez que este regime carece urgentemente de alterações, que o tornem adequado à realidade de hoje em dia. Contudo, e como veremos agora, não foi esse o cerne desta proposta de lei, que acabou por ser declarada inconstitucional pelo Tribunal Constitucional, uma vez que exacerbava os problemas já constantes da redação atual. É importante a análise da lógica do Tribunal Constitucional, subjacente à decisão, mas mais importante ainda se afigura a análise das grandes questões suscitadas, e eixos constitucionais invocados no âmbito deste tipo de apreensões, de modo a reiterar a necessidade de tutela deste tipo de métodos de obtenção de prova, ainda que o legislador tenda a as desproteger face aos meios de obtenção de prova tradicionais.

a. Principais mudanças de regime e implicações inerentes

Sobre as alterações em causa e quanto às formalidades exigíveis para apreensão do correio eletrónico ou semelhante podemos referir duas grandes alterações: quanto ao órgão competente e quanto à própria definição do objeto das apreensões.

Quanto à primeira alteração, na versão atual a competência exclusiva é do juiz, já na versão proposta a competência pertence à "autoridade judiciaria competente". Daqui resulta a possibilidade de esta autoridade ser o MP ou mesmo até (17, n°2) OPCs, ou o juiz, dependendo da fase processual em questão.

[59] Neste capítulo acompanhamos de perto a análise efetuada pelo Tribunal Constitucional (acórdão 687/2021).

O n°4 desta nova redação é bastante semelhante ao nº3 do artigo 179. ° do CPP, que também atribui ao juiz competência para determinar a junção da correspondência apreendida a processo.

Por outro lado, os órgãos de polícia criminal podem apreender correio eletrónico ou similar nas situações de pesquisa informática executada nos termos do artigo 15º da própria Lei do cibercrime, ou quando haja urgência ou perigo na demora, exigindo-se ulterior validação pela autoridade judiciária no prazo máximo de 72 horas.

Em coerência com o estabelecido nos artigos 55º e 249º do CPP quanto à competência dos Órgãos de Polícia Criminal, a estes é atribuída a faculdade de praticar, no âmbito da apreensão de correio eletrónico os atos destinados a assegurar os meios de prova, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do ártigo15.º, bem como (o que parece indiciar uma condição alternativa e não cumulativa) nos casos de urgência ou perigo na demora - atos estes sujeitos, como sempre se imporia, a subsequente validação da autoridade judiciaria.

Nestes termos, não só o Ministério Público passa a ter, em fase de inquérito, e à luz da nova redação do n.º 1, competência para uma intervenção prévia à apreensão - ordenando-a ou autorizando-a, por despacho, em vez do Juiz de Instrução Criminal -, como o n.º 2 do mesmo artigo admite também uma intervenção depois do facto, validando, no prazo de 72 horas, a apreensão realizada pelo Órgão de Polícia Criminal.

É importante ainda, notar que nenhuma destas normas propostas preveem um prazo para validação pelo juiz, quando ordenadas pelo MP, ou validação pelo próprio quando feitas pelos OPC.

Quanto à própria definição do objeto das apreensões na versão atual podem ser apreendidas mensagens de correio eletrónico, ou semelhante, que se revelem de grande interesse para a descoberta da verdade ou para a prova. Já na versão proposta alarga-se o objeto a todo o conjunto de mensagens necessárias à produção de prova, tendo em vista a descoberta da verdade. Tratar-se-ia de uma ponderação que poderia ser feita por qualquer dos órgãos com competência para efetuar a apreensão.

Note-se, ainda, que a remissão em bloco para o artigo 179º, passou a ser na versão proposta uma previsão de aplicação subsidiaria, com as necessárias adaptações. No entanto, o legislador inspira-se no disposto no n.º 3 do artigo 179º do CPP quando, no

(novo) n.º 4 do artigo 17º estabelece que caberá ao juiz aferir da pertinência da junção a processo das mensagens apreendidas. Este paralelismo é importante porque estende a correio eletrónico uma das mais relevantes garantias em situações de apreensão de correspondência - a consagração da nulidade como sanção associada à ausência de despacho do juiz (179/1)

Assim, em causa parece estar efetivamente um regime jurídico autónomo, com paralelismos significativos com o regime consagrado no artigo 178º relativo às apreensões de objetos relacionados com a prática de um facto ilícito típico, deixados pelo agente no local do crime ou quaisquer outros suscetíveis de servir de prova.

No fundo, esta versão proposta do artigo 17º, constrói-se, para a específica situação de apreensão de correio eletrónico ou similar, um regime híbrido, que combina elementos significativos do regime consagrado no artigo 178. ° do CPP, com o regime do artigo 179º.

O novo regime implica um reforço da competência do MP em fase de inquérito, reservando a intervenção do juiz para a apreensão de mensagens de correio eletrónico ou semelhantes para a eventual junção aos autos.

1. Conjugação com a jurisprudência internacional europeia

O Tribunal Constitucional considerou que a lei 109/2009 deveria, necessariamente, ser interpretada à luz do contexto normativo quer da União Europeia, quer do conselho da europa, atendendo as standards de proteção que deles resulta para os direitos fundamentais aqui em causa designadamente, a privacidade, entendida em sentido lato, e com particular relevância do domínio da proteção de dados e utilização da informática.

O Tribunal de Justiça da União Europeia (TJUE) e o Tribunal Europeu dos Direitos do Homem (TEDH) oferecem jurisprudência interessante e muito relevante neste âmbito.

A matéria em causa suscita a invocação dos artigos 7º, 8º, e 52, nº1 da Carta dos Direitos Fundamentais da União Europeia (CDFUE) que consagram respetivamente: i) O direito de todas as pessoas ao respeito pela sua vida privada e familiar, pelo seu domicilio e pelas sus comunicações; ii) o direito de todas as pessoas à proteção dos dados de caracter pessoal que lhes digam respeito – os quais devem ser objeto de um tratamento leal, para

fins específicos e e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, ficando o cumprimento destas regras sujeito a fiscalização por parte de uma autoridade independente; e iii) a garantia de que qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela CDFUE deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades, na observância do princípio da proporcionalidade, o que implica que essas restrições só possam ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros. A proteção dos dados pessoais é, além disso, um direito fundamental igualmente consagrado no artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia ("TFUE").

Assume, por último, relevância a consagração no artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais ("CEDH"), do direito de qualquer pessoa ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

A nível europeu a jurisprudência oferece certas linhas orientadoras. No que toca a direitos fundamentais das medidas de conservação de dados, a interpretação combinada dos direitos à privacidade e à proteção de dados, que estão indissociavelmente ligados. Esta combinação aparece, então, como standard de proteção aplicável quando estão em causa dados de um processo de comunicação entre pessoas que se situem na sua esfera privada.

2. Conjugação com a jurisprudência constitucional[60]

[60] Acórdão n.º 241/2002;
Acórdão n.º 464/2019;
Acórdão n.º 486/2009;
Acórdão n.º 403/2015;
Acórdão n.º 464/2019;
Acórdão n.º 23/90;
Acórdão nº 395/2004 (posição que seria ainda reafirmada no Acórdão n.º 67/2006;
Acórdãos n.º 155/2007 e n.º 228/2007;
Acórdão n.º 387/2019;
Acórdão n.º 121/2021

A nível da jurisprudência do Tribunal Constitucional, podemos identificar dois polos fundamentais suscitados pelo Tribunal.

Por um lado, a tutela jurídico-constitucional da privacidade, da correspondência, telecomunicações e dos dados informáticos; e por outro, a divisão de competências, no que respeita a diligências efetuadas em sede de inquérito, entre Ministério Público e Juiz de Instrução Criminal, com particular atenção à especial garantia constitucional respeitante a atos que se prendam diretamente com direitos fundamentais.

Quanto ao primeiro polo, o Tribunal Constitucional[61] refere o artigo 28º, nº1 que reconhece o "direito à reserva da intimidade da vida privada", o artigo 34º, que garante a inviolabilidade do "sigilo da correspondência e dos outros meios de comunicação privada" (nº1) e proíbe "toda a ingerência das autoridades públicas (…) nas telecomunicações e nos demais meios de comunicação salvo os casos previstos na lei em processo criminal" (nº4) e do artigo 32º, nº8 que, no âmbito das garantias do processo criminal, fulmina com a nulidade "todas as provas obtidas mediante (…) abusiva intromissão na vida privada, no domicilio, na correspondência ou nas telecomunicações".

Determina o tribunal que resulta da proteção constitucional reforçada atribuída à correspondência, telecomunicações os outros meios de comunicação privada, que decorre do artigo 34º, n.ºs 1 e 4, da CRP, que a intenção do legislador constituinte foi a de limitar significativamente possibilidade e a amplitude quer de restrições legais, quer de atuações restritivas das autoridades públicas, em tais domínios.

Mais, afirma o tribunal que a proteção constitucional das "telecomunicações" abrange um vasto leque de dados sobre comunicação humana, não apenas os de conteúdo, apesar de, obviamente, a proteção constitucional oferecida ao conteúdo material ser sempre mais intensa que a oferecida aos chamados *metadados* no geral – isto releva pois o tribunal afasta desde logo a possibilidade de se afastar a jurisprudência e argumentos invocados por em causa estarem em causa dados de conteúdo e não dados de tráfego, especialmente tendo em conta que é pacifico na doutrina e jurisprudência que ambos se incluem no âmbito de proteção do artigo 34°, n°4.

[61] Ainda no acórdão 687/2021

Já no plano de proteção da comunicação humana, importa referir que entendeu o tribunal que é vedada possibilidade de restrições dos direitos fundamentais a elas atinentes - *exceto quando tais restrições se situem no âmbito do processo penal*. Fala-se aqui numa reserva absoluta de processo criminal.

O Tribunal Constitucional invoca um outro acórdão[62], que defende que o nº4 do artigo 34º da CRP protege tanto o processo comunicativo como o conteúdo da comunicação, sendo apenas relevante para o efeito que tenha havido um efetivo processo comunicativo – ou seja, a consciência e vontade de pelo menos uma das partes em transmitir dados ou noticias à distância. Esta tese é sustentada pela doutrina e jurisprudência alemãs, que já enfatizou a necessidade de proteção efetiva dos dados de conexão no âmbito de proteção dos diretos fundamentais – como veremos adiante.

Por fim, aborda, o tribunal, a questão da autodeterminação informativa (que iremos também tratar no próximo capítulo) - que se prende com o direito de cada um controlar as informações que lhe dizem respeito, que são pessoais e recolhidas e tratadas por entidades publicas e privadas cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas, - e distingue- a da autodeterminação comunicativa que, por sua vez, se reporta as comunicações individuais efetivamente realizadas ou tentadas que são as únicas que estão, de facto, cobertas pelo sigilo de comunicações.

No âmbito do segundo polo, relativo à divisão de competências, o Tribunal Constitucional tem-se mantido coerente ao longo dos anos, nunca tendo hesitado, perante uma intervenção restritiva de direitos fundamentais, em afirmar a necessidade absoluta de intervenção prévia do juiz de instrução.

Mantém, ainda, que a intervenção do juiz no inquérito, em relação a atos que sejam restritivos de direitos fundamentais do arguido, é um pilar incontornável do processo penal português, como decorre do artigo 32º, nº4 da CRP.

Na mesma linha, Figueiredo Dias, citado pelo Tribunal Constitucional, também defende que atos processuais que atinjam diretamente direitos, liberdades e garantias, competem necessariamente ao juiz de instrução criminal durante o inquérito.

---

[62] Acórdão nº 403/2015

No entanto, é evidente que a articulação da ação penal do MP e a competência do JIC que consiga conjugar adequadamente o princípio do acusatório e a competência exclusiva do juiz para a prática de atos que afetem direitos fundamentais, foi alvo de inúmeras pronúncias. Uma delas, por exemplo, determina o monopólio do juiz-garante dos direitos dos cidadãos, que se restringe, no entanto, precisamente a esse núcleo de garantia constitucional.

Assim cabe toda a fase de inquérito ao MP, nos termos do artigo 262°, n°1 CPP, justificando-se apenas, a intervenção garantística de um juiz sempre que esse núcleo seja afetado, consoante o elenco de situações descritas nos artigos 268° e 269º.

No fundo, o Tribunal Constitucional parece entender, e bem, que para aferir da constitucionalidade da proposta de lei em causa, é necessário compreender os direitos constitucionalmente protegidos em jogo – os que já são afetados ou postos em causa pelo regime atual, e que se veriam ainda mais atingidos por uma alteração ao mesmo que, no mais, parece exponenciar facilitismos e a desproteção que já caracteriza o regime.

Deste modo, aprofundemos agora algumas considerações finais, e poderemos qual deveria ser o caminho a seguir pelo legislador no âmbito desta matéria tendo em conta todas as contingências que têm vindo a ser apontadas neste estudo.

VI. Considerações finais – a inconstitucionalidade do regime proposto e considerações para o futuro.

Chegados a este ponto parecem evidentes as implicações constitucionais destes regimes (de buscas informáticas e de apreensão dos dados informáticos); porém, optamos por expor certos aspetos que revestem particular importância.

Começando pela dignidade humana, ponto de partida de todo o catálogo de direitos fundamentais, podemos afirmar que hoje em dia este direito tem reflexões a nível da privacidade e da reserva da vida privada. O Tribunal Constitucional já assim entendeu[63], determinando que a reserva da vida privada é uma condição da integridade da pessoa e a sua proteção deve ser considerada como um aspeto de proteção da dignidade humana.

[63] Acórdão nº 263/97

O direito à reserva da vida privada "tutela, essencialmente, o interesse de cada pessoa em controlar a informação sobre a sua vida privada, impedindo que terceiros possam, sem o seu acordo, tomar conhecimento ou divulgar essa informação"[64].

O acórdão do Tribunal Constitucional nº 278/95 constata que a Constituição não estabelece o conteúdo mínimo do direito à reserva da intimidade, nem define o conceito de intimidade em si mesmo. Tal conceito aberto não é estranho à Lei Fundamental, o que permite que os conceitos e o núcleo essencial dos direitos não fique parado no tempo, sendo necessárias sucessivas alterações à Constituição para incorporar conceitos novos. A verdade é que em virtude da velocidade a que a tecnologia e a sociedade evoluem, são essenciais conceitos flexíveis. A este respeito Paulo Mota Pinto (1999) referiu que esta perspetiva permite a tutela de novos bens e faz face a renovadas ameaças à pessoa humana.

A ideia da privacidade, ou da reserva da vida privada ligada à evolução tecnológica, e às ingerências nas comunicações eletrónicas, não é, no entanto, nova. Já nos anos 70 se falava na necessidade de "proteger a vida privada face às possibilidades criadas pelo uso de meios informáticos para a obtenção de informações sobre os indivíduos.[65]". A resolução nº 428 da Assembleia Parlamentar do Conselho da Europa[66] mostrava esta preocupação: "Quando sejam implementadas bases de dados regionais, nacionais, ou internacionais o individuo não pode ficar completamente exposto e transparente pela acumulação de informações, nomeadamente sobre a sua vida privada." E se tal já se demonstrava uma verdade absoluta à data, hoje ainda mais o é.

Catarina Sarmento e Castro (2005) aborda a obra de dois autores norte-americanos - Samuel Warren e Louis Brandeis - que nos anos 90, defenderam[67] pela primeira vez o direito uma refelxão do direito à privacidade que intitularam o "right to be left alone" – o direito de ser "deixado em paz" ou "direito de ser deixado sozinho"[68]. Este direito é um

---

[64] PINTO, 2005

[65] SARMENTO E CASTRO, 2005

[66] Disponível em https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en

[67] Warren, Samuel / Brandeis, Louis, « The right to privacy», Harvard Law Review, Vol. IV, nº5, 15 de December 1890, p.193 e ss.

[68] Tradução nossa.

direito contra o mundo, como exposto pelos autores. Rapidamente este "right to privacy" foi tido como uma importante e abragente aceção da personalidade humana.

A nossa Constituição prevê o Direito à reserva da vida privada no artigo 26.º, n.º 1, complementando com o artigo 34º sobre a inviolabilidade do domicílio e da correspondência, bem como no artigo 35º, nºs 1 e 4, relativo à proteção dos dados pessoais no âmbito da utilização da informática.

O direito à reserva da vida privada é, no fundo, um direito sobre informação "relativo à projeção vital da personalidade, que engloba uma esfera privada, uma esfera mais restrita, a pessoal, uma esfera de segredo (pessoal ou não) e um direito à solidão (o "right to be let alone")"[69].

Já o artigo 35º se traduz num

> "(…) feixe de prerrogativas que pretendem garantir que cada um de nós não caminhe nu, desprovido de um manto de penumbra, numa sociedade que sabe cada vez mais acerca de cada indivíduo. É um direito a não viver num mundo com paredes de vidro, é um direito a não ser transparente, por isso, desenha-se como um direito de proteção em sentido negativo. Visto deste prisma, o direito em causa permite que o indivíduo negue informação pessoal, se oponha à sua recolha, difusão ou qualquer outro modo de tratamento Neste sentido, aproxima-se da ideia americana de "privacy", enquanto direito de defesa face às agressões do Estado e terceiros às suas informações pessoais. Mas é mais (…) é um direito a decidir até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam, construindo-se como uma liberdade, como um poder de determinar o uso dos seus dados pessoais."[70].

Este direito relativo à proteção dos dados pessoais no âmbito da utilização da informática é uma manifestação da importância que revestem os dados que se guardam em ambiente digital, e da necessidade da sua tutela especializada e adequada aos dias de hoje.

[69] SARMENTO E CASTRO, 2005

[70] SARMENTO E CASTRO, 2005

Quanto à inviolabilidade da correspondência e das comunicações (consagrada no artigo 34. °, n.º 1, da CRP) também já é clara a sua relevância no âmbito das buscas e apreensões em ambiente informático, em especial no que concerne ao artigo 17º da LC.

Vânia Costa Ramos (2006) diz, relativamente a um acórdão do BVerfG (*supra* citado) que "o segredo das comunicações garante o direito ao livre desenvolvimento da personalidade através do intercâmbio de informações privado, subtraído à esfera pública." De facto, o BVerfG tem entendido, na linha do que temos vindo a defender, que

> "(…) a digitalização tem por consequência a circunstância de que cada comunicação, mesmo terminada, deixar marcas, suscetíveis de serem gravadas e valoradas. O direito fundamental ao sigilo de comunicações protege, pois, de igual modo, os detalhes da comunicação – saber se, quando e quantas vezes houve, ou foi tentada , comunicação entre que pessoas ou aparelhos – uma vez que tais detalhes possuem em si mesmos, valor declaratório. De outro modo, a proteção conferida pelo sigilo das comunicações seria insuficiente.".[71]

No fundo, tal como já era evidente, estes regimes têm elevadas implicações a nível constitucional. No entanto, "(…) há que ter em conta que nenhum dos direitos fundamentais tem valor absoluto, devendo ceder para salvaguardar outros direitos fundamentais que sejam mais relevantes na situação concreta (…)"[72]. Ainda assim, quanto ao regime em vigor temos dúvidas acerca da proporcionalidade, necessidade e adequação de certas restrições dos direitos fundamentais em causa, em prol do combate - não só ao cibercrime– mas a todo o tipo de criminalidade, desde que exista algum tipo de prova a recolher em ambiente informático. Quanto ao regime proposto, no entanto, não temos dúvidas que os direitos fundamentais acima referidos fossem postos em causa desmesuradamente.

Nesta linha, e *a final*, o Tribunal Constitucional acabou por pugnar pela inconstitucionalidade do regime proposto.

Vejamos:

---

[71] COSTA RAMOS, 2006

[72] SILVA RODRIGUES, 2009

O Tribunal Constitucional, comparando, mais uma vez, a versão atual e a versão proposta para o artigo 17º, afirma que esta última consagra uma solução legal que possibilita a apreensão de mensagens de correio eletrónico que sejam conhecidas no decurso de uma medida de investigação criminal validamente determinada.

Sobre esta base, e face a tudo o que já foi exposto, é necessário compreender certos pontos assentes pelo TC.

Levantam-se várias dúvidas interpretativas sobre se este regime ficará como regime regra para as tais mensagens ou se com regime subsidiário para situações concretamente determinadas, aplicando-se, de resto, o disposto no artigo 179º do CPP. Independentemente dessa questão, em causa estarão sempre todas as mensagens encontradas e não atuando apenas em circunstâncias de especial urgência ou perigo em demora que exijam atuação cautelar. Sendo certo que se este regime se aplica a uma parte significativa de apreensões de correio eletrónico, uma vez que é provável que a maior parte das pesquisas em sistemas informáticos revelem a existência de mensagens de correio eletrónico.

Não é feita qualquer delimitação do âmbito de aplicação em função da gravidade da ação criminosa ou da moldura penal em causa, o que é agravado por este regime se aplicar não só às mensagens encontradas ou armazenadas no sistema informático objeto de pesquisa, mas em qualquer outro a que seja permitido acesso legitimo a partir do primeiro, alargando significativamente o perímetro de localização das mensagens.

Não é inequívoco que a sua aplicação se restrinja a comunicações já efetuadas e não aquelas que possam ainda estar a decorrer.

O correio eletrónico é uma realidade complexa, que convoca elementos relativos quer à tutela das telecomunicações, quer à proteção da correspondência postal, e em causa estarão dados de conteúdo, analogamente aos que estão em causa na correspondência, mas também dados de tráfego, em termos muito mais amplos. Estes últimos, mesmo que não se aceda propriamente aos dados de conteúdo das mensagens eletrónicas, já são em si mesmos suscetíveis de revelar várias informações relevantes para aferir que mensagens serão mais importantes requerer a um juiz que se juntem aos autos -fala-se aqui de dados como os destinatários, a existência de anexos, as horas, a data o IP de origem, o volume de dados transmitidos, o assunto da mensagem...etc.

Identifica bem o tribunal, que o que sucederá na maior parte dos casos será que na escolha das mensagens a apresentar ao juiz tenha que ser feita uma pré seleção, precisamente com base nestes dados de trafego, e com recurso a buscas de palavras-chave, pelo que é certo que mesmo que estas normas questionadas não transformem a intervenção em direitos fundamentais aqui em causa num espaço live de controlo jurisdicional, tal não significa que não se crie um espaço para apreensões abusivas, nem tomada de conhecimento indevido de dados de trafego relativos ao correio eletrónico de eventuais arguidos ou terceiros, por parte do MP e dos OPC. E a questão densifica-se quando se pensa que não existe verdadeiramente uma reversão destas intervenções abusivas - o que foi visto não vai deixar de ter sido visto, ao contrário do que acontece com objetos indevidamente apreendidos que podem simplesmente ser devolvidos a legitimo proprietário.

O n°2 do mesmo artigo consagra na verdade uma regulamentação paralela à do n°1, sendo que se o MP tiver legitimamente ordenado a pesquisa, os OPC podem por si só efetuar a apreensão, sendo esta posteriormente validada pelo MP sem intervenção necessária do JIC.

Isto significa que em causa está um regime regra que em condições de normalidade e previsibilidade do decurso do processo penal regerá a apreensão de mensagens de correio eletrónico, e é neste contexto que se deve avaliar o potencial de inconstitucionalidade.

Quanto aos direitos fundamentais, remetemos para as observações supra descritas, deixando apenas nota que a proteção constitucional conferida à correspondência privada compreende todas as variantes de correspondência entre indivíduos, no geral, quaisquer formas de comunicação humana de carácter privado, no âmbito do artigo 34º, nº4 da CRP e o facto é que as normas em apreciação permitem a ingerência na correspondência eletrónica, possibilitando também o conhecimento de uma série de dados pessoais, quer de tráfego quer de conteúdo, abrangidos pela garantia constitucional de inviolabilidade do sigilo a correspondência.

É possível afirmar, com base nas razões expostas, que o novo regime do artigo 17º da Lei do Cibercrime constitui, conjuntamente com o artigo 16°, o núcleo duro da disciplina normativa do acesso a dados de natureza informática no âmbito do processo penal, eliminando, ao contrário do artigo 16.º, a exigência de intervenção primária do JIC, bem como a de este ser o primeiro a ter conhecimento do conteúdo das mensagens apreendidas.

Sendo razoável afirmar também, como o faz o tribunal, que hoje em dia os sistemas informáticos têm um papel predominante na vida pessoal de cada um, e por isso, a pesquisa do seu conteúdo constitui necessariamente uma intrusão da vida privada, de tal forma grave que , na opinião do TC, é necessário assegurar nestes domínios o cumprimento do dever estadual de abstenção, ou não ingerência, a não ser em casos excecionais, rigorosamente delimitados e justificados, mediante a atuação de órgãos que assegurem a intervenção isenta e imparcial, e ainda um elevado grau de proteção dos direitos fundamentais afetados, uma vez que o potencial para lesões de direitos fundamentais nessa matéria é, de facto, elevadíssimo.

O processo penal surge como o único âmbito em que uma restrição de direitos fundamentais deste tipo poderia suceder (reserva absoluta do processo penal), por haver fundamento bastante para permitir restrições legais e intervenções restritivas por parte de autoridades públicas. No entanto, há sempre que salvaguardar o modo admissível de o fazer, não deixando de assegurar os direitos fundamentais das pessoas, as garantias de defesa dos arguidos e a presunção de inocência, e proibição de provas obtidas mediante intromissão na vida privada, no domicilio e na correspondência ou nas telecomunicações, bem como, não deixando de assegurar a competência de um juiz para a pratica de atos instrutórios que se prendam com direitos fundamentais.

Apesar de, no âmbito do processo penal, estarmos já perante um contexto em que há notícia de crime, não se pode deixar de analisar atentamente o cumprimento das exigências de excecionalidade, determinabilidade e proporcionalidade.

Quando está em causa uma atuação restritiva das autoridades publicas no âmbito dos direitos fundamentais, a intervenção de um juiz independente e imparcial é essencial para uma tutela efetiva desses direitos, mesmo nos casos em que estes devam parcialmente ceder em nome da salvaguarda de outros bens constitucionalmente protegidos.

E a intervenção do Juiz de Instrução Criminal não pode, atentas as normas constitucionais e legais que a regem, ser olhada como um "obstáculo à produção de prova". Estando a atribuição da competência para a determinação ou autorização da apreensão de correio eletrónico ou de natureza semelhante, afeta ao JIC, na dependência de requerimento do Ministério Público, ela não colide com a direção e o domínio do inquérito por esta entidade.

Ainda que não se duvide de que os interesses prosseguidos pela investigação criminal constituem razões legítimas para uma afetação restritiva dos direitos fundamentais à inviolabilidade da correspondência e sigilo das comunicações e à proteção dos dados pessoais, no domínio da utilização da informática, essas restrições nunca podem deixar de respeitar os princípios fundamentais e condições impostas pela constituição. nem tão pouco, a exigência especifica de intervenção de um juiz, consagrada no artigo 32.º, n° 4, da CRP.

Concluiu o tribunal que a norma objeto do recurso é inconstitucional, por violação dos direitos fundamentais à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.°, n.º 1, da CRP), à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.°, n.ºs 1 e 4, da CRP), enquanto refrações específicas do direito à reserva de intimidade da via privada, (consagrado no artigo 26.9, n.º 1, da Constituição), em conjugação com o princípio da proporcionalidade (nos termos do artigo 18.°, n.º 2, da CRP) e com as garantias constitucionais de defesa em processo penal (previstas no artigo 32.º, n.º 4, da Lei Fundamental).

Face a esta conclusão é evidente que esta alteração ao artigo 17º da Lei do Cibercrime com vista a melhorar a "eficácia e eficiência" (como consta do projeto lei) fá-lo em claro prejuízo dos direitos fundamentais dos cidadãos, não se assegurando as garantias mínimas de defesa no âmbito do processo penal.

Assistimos, com esta tentativa, em última análise, a uma crescente desproteção do arguido, em absoluto, mas também de qualquer visado pelo meio de obtenção de prova. Atualmente, porém, a sociedade evolui digitalmente num caminho de elevada vulnerabilidade de todos os cidadãos, em que a privacidade é um direito fundamental, mas uma realidade escassa, em que apesar de toda a preocupação com o tratamento de dados pessoais, estes são vendidos como moeda de troca. O Estado impõe-se, então, como a primeira linha de defesa contra os ataques diários a estes direitos, e não como um entrave à sua plena realização.

Uma das alterações fundamentais deste projeto prendia-se com o afastamento da necessidade de autorização prévia de um juiz de instrução criminal para este tipo de apreensão, e uma das críticas do Tribunal Constitucional, como vimos, relaciona-se precisamente com esta questão: que o papel do Juiz não pode ser visto como um entrave

ao exercício do Ministério Público, muito pelo contrário, e a realidade é que parece preocupante ser esse o caminho por onde se pretende enveredar.

Nas palavras de Renato Militão (2012), "facilitar, amplificar, agilizar medidas de criminal no domínio da obtenção de prova digital torna-se ainda mais agressivo, intrusivo, desleal e perigoso do que fazê-lo em relação às 'provas tradicionais'", e de facto, é crucial haver um cuidado acrescido a legislar sobre este tipo de métodos de obtenção de prova.

Várias foram as críticas tecidas à atual redação dos regimes das buscas e apreensões informáticas. No entanto, a crítica mais pertinente será talvez afirmar que os regimes em causa não são adequados a satisfazer as necessidades dos dias de hoje. Não só não são adequados, como o modo como o fazem também é em si mesmo desadequado a proteger os direitos fundamentais dos envolvidos. Assim, urge a criação de um regime autónomo, livre das dúvidas que enfermam o atual regime, mas que não pretenda exacerbar as falhas de um regime que Benjamim Silva Rodrigues (2009) apelida de "terrorismo estadual ao nível do direito à autodeterminação informacional."

"A proteção de direitos fundamentais é uma inquestionável finalidade primária do próprio processo penal, que ficou demasiado fragilizada."[73].

Resulta do nosso estudo, então, que é essencial um regime que preveja procedimentos especificados para garantir a boa recolha de prova em ambiente digital e que determine, nomeadamente, a necessidade de um despacho judicial prévio.

[73] COSTA ANDRADE, 2009

VII. Referências bibliográficas

ALBUQUERQUE, Paulo Pinto de Comentário do Código de Processo Penal: *à luz da Constituição da República e da Convenção dos Direitos do Homem*, 4.ª Edição, Universidade Católica Editora, 2011;

ANDRADE, Manuel da Costa, "Sobre o regime processual penal das escutas telefónicas", *Revista Portuguesa de Ciência Criminal*, Ano I, 3, Jul/Set, 1991, Aequitas, p. 369-408;

ANDRADE, Manuel da Costa, *Bruscamente no verão passado, A reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009;

ANDRADE, Manuel da Costa, *Sobre as proibições de prova em Processo Penal*, Reimpressão, Coimbra Editora, 2013;

BAILIE, Michael W.; HAGEN, Ed; JARRET, H. Marshall, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, s.n, s.l, 2009, consultado em: 04-05-2016.

CANOTILHO,J. J. Gomes; MOREIRA, Vital, *Constituição da República Portuguesa anotada*, Vol. I, 4.ª Edição Revista, Coimbra Editora, 2014;

CARDOSO, Rui, Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX - *Curso CEJ 2021*

CASTANHEIRA NEVES, Rita, *As Ingerências nas Comunicações Electrónicas em Processo Penal - Natureza e Respectivo Regime Jurídico do Correio Electrónico Enquanto Meio de Obtenção de Prova*, s.l., Coimbra Editora, 2011.

CASTRO, Catarina Sarmento e, *O direito á autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro*, Estudos de Homenagem ao Conselheiro José Manuel Cardoso da Costa, Vol. II, Coimbra Editora, 2005, p. 65-95;

CORREIA, João Conde, "Prova Digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público nº 139,* Ano 35, Junho- Setembro 2014.

CORREIA, João Conde, “Prova digital: as leis que temos e a lei que devíamos ter”, *Revista do Ministério Público*, n.º 139, Jul/Set, 2014, p. 29-59;

COSTA, José de Faria, *As telecomunicações e a privacidade: o olhar (in)discreto de um penalista*, Direito Penal da Comunicação – Alguns escritos, Coimbra Editora, 1998, p. 47- 78;

DIAS, Jorge de Figueiredo, “Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa)”, *Revista de Legislação e de Jurisprudência, n.º 146*, 2016, p. 3 a 16; 62

ETZIONI, Amitai, *Privacy in a Cyber Age*, Palgrave Macmillan, New York, 2015, pp. 132/133

FARMER JR., John J. - *Computer Evidence Search* & Seizure Manual, Department of Law & Public Safety Division of Criminal Justice, New Jersey, 2000

FIDALGO, Sónia, “Apreensão de correio eletrónico e utilização noutro processo das mensagens apreendidas”, *Revista Portuguesa de Ciência Criminal*, n.º 1, IDPEE, 2019, p. 59-74;

MARTINS, A. G. Lourenço, *Criminalidade informática*, AA.VV., Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, 2003, p. 9-41;

MARTINS, A. G. Lourenço; MARQUES, J. A. Garcia; DIAS, Pedro Simões, *Cyberlaw em Portugal: O direito das tecnologias da informação e da comunicação*, Centro Atlântico, 2004;

MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, s.l., Coimbra Editora, 2010.

MESQUITA, Paulo Dá, *Prolegómenos sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português* – o Código e a Lei do Cibercrime, Processo Penal, Prova e Sistema Judiciário, Coimbra Editora, 2010, p. 83-129;

MILITÃO, Renato Lopes, A *Propósito da Prova Digital no Processo Penal*, s.l., s.n.

NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal, Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra Editora, 2011

NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018;

PINTO, Ana Luísa, "As buscas não domiciliárias no direito processual penal português", *Revista do Ministério Público*, Ano28, n.º 109, Janeiro- Março 2007.

PINTO, Ana Luísa, "Aspectos Problemáticos do Regime das Buscas Domiciliárias", *Revista Portuguesa de Ciência Criminal*, Ano 15, n.º 3, 2005.

RAMALHO, David Silva, A recolha de prova em sistemas de computação em nuvem", in *Revista do Direito Intelectual* , N.º 2, 2014, p. 142-146.

RAMALHO, David Silva, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017;

RAMOS, Armando Dias, A *prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017;

RAMOS, Vânia Costa, "Âmbito e Extensão do Segredo das Telecomunicações (Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, 2 de março de 2006)", *Revista do Ministério Público*, n.º 11, Out./Dez., 2007, p. 141- 159;

RODRIGUES NUNES, Duarte, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, Coimbra, 2018, p. 140).

RODRIGUES, Benjamim Silva, Da Prova Penal – Tomo IV, Da Prova- *Electrónico Digital e da Criminalidade Informático-Digital*, 1ª Edição, s.l., Rei dos Livros, 2011.

RODRIGUES, Benjamim, *Das escutas telefónicas – À obtenção da prova [em ambiente] digital*, Tomo II, 2.ª Edição, Coimbra Editora, 2009;

RODRIGUES, Benjamim, D*ireito penal, Parte especial – Direito penal informático-digital*, Tomo I, Coimbra Editora, 2009; 63

VENÂNCIO, Pedro Dias, "As Medidas de Prova Digital da Lei do Cibercrime- regra ou exceção", *Boletim da Ordem dos Advogados, nº 23*, Fevereiro, 2015

VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada, 1ª Edição*, s.l. Coimbra Editora, 2011.

VENÂNCIO, Pedro Dias, *Lei do cibercrime anotada e comentada*, Coimbra Editora, 2011;

VERDELHO, Pedro, "A Nova Lei do Cibercrime", *Boletim da Ordem dos Advogados*, nº 65, Abril, 2010, pp 34-35.

VERDELHO, Pedro, "A nova lei do cibercrime", *Scientia Iuridica*, Tomo LVIII, n.º 320, 2009, Universidade do Minho

VERDELHO, Pedro, "A obtenção de prova no ambiente digital", *Revista do Ministério Público*, Ano 25, n.º 99, 2004.

VERDELHO, Pedro, Cibercrime, AA.VV., *Direito da sociedade da informação*, Vol. IV, Coimbra Editora, 2003.

Warren, Samuel / Brandeis, Louis, « The right to privacy», *Harvard Law Review*, Vol. IV, nº5, 15 de December 1890, p.193 e ss [Original source: https://studycrumb.com/alphabetizer]

Outras Fontes

Minuta Relatório Explicativo da Convenção do Cibercrime em Português, consultado em 19-04-2016, disponível em http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf.

Proposta de Lei n.º 289/X/4ª https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=34566

https://datareportal.com/reports/digital-2022-portugal

Jurisprudência consultada:

Tribunal Constitucional

Acórdão 687/2021, disponível em www.dgsi.pt

Acórdão n.º 241/2002, disponível em www.dgsi.pt

Acórdão n.º 464/2019, disponível em www.dgsi.pt

Acórdão n.º 486/2009, disponível em www.dgsi.pt

Acórdão n.º 403/2015, disponível em www.dgsi.pt

Acórdão n.º 464/2019, disponível em www.dgsi.pt

Acórdão n.º 23/90, disponível em www.dgsi.pt

Acórdão nº 395/2004, disponível em www.dgsi.pt

Acórdão n.º 155/2007, disponível em www.dgsi.pt

Acórdão nº 228/2007, disponível em www.dgsi.pt

Acórdão n.º 387/2019, disponível em www.dgsi.pt

Acórdão n.º 121/2021, disponível em www.dgsi.pt

Acórdão nº 403/2015, disponível em www.dgsi.pt

Acórdão nº 263/97, disponível em www.dgsi.pt

Supremo Tribunal de Justiça

Acórdão do STJ de 26 de Novembro de 1992, disponível em www.dgsi.pt

Acórdão do STJ de 11 de Março de 1993, disponível em www.dgsi.pt

Acórdão do STJ de 8 de Fevereiro de 1995, disponível em www.dgsi.pt

Acórdão do STJ de 5 de Junho de 1991, disponível em www.dgsi.pt

Tribunais da Relação

Acórdão do TRC de 10 de Julho de 1991, disponível em www.dgsi.pt

Acórdão do Tribunal da Relação de Lisboa de 29-12-2017, disponível em www.dgsi.pt

Acórdão do Tribunal da Relação de Guimarães de 29-03-2011, disponível em www.dgsi.pt

Acórdão do Tribunal da Relação de Lisboa de 11-01-2011, disponível em www.dgsi.pt

Acórdão do Tribunal da Relação de Lisboa de 29-12-2017, disponível em www.dgsi.pt

Acórdão do Tribunal da Relação de Lisboa de 06-02-2018, disponível em www.dgsi.pt

Jurisprudência internacional

United States v. Matlock, 415 U.S. 164 (1974)

BVerfG, 2 BvR 2099/04 de 02.03.2006, nº(1-142), disponível em https://www.bundesverfassungsgericht.de/entscheidungen/rs20060302_2bvr209904.html

Acórdão do Tribunal de Justiça (grande secção) de 8 de Abril de 2014 (casos C-293/12 e C-594/12).